Mutual Evaluation of Türkiye

Anti-money laundering and countering the financing of terrorism and proliferation financing measures



September 2026



The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit www.fatf-gafi.org.

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

How to read this mutual evaluation report

The Financial Action Task Force (FATF) has revised its assessment methodology to place an even greater focus on effectiveness, to ensure that countries are implementing and making use of the laws, regulations and policies that are being passed, as well as a greater emphasis on the major risks and context. This round of mutual evaluations is operating on a six-year cycle, significantly shorter than earlier rounds, and includes time-bound Key Recommended Actions roadmaps for countries that need to improve in key areas.

Effectiveness has been assessed according to the 11 immediate outcomes that an effective anti-money laundering/countering the financing of terrorism/countering proliferation financing (AML/CFT/CPF) framework should be able to deliver. The extent to which a country is taking effective action in this area is reflected in ratings that range from low to high level of effectiveness (see Chapters 2 – 11).

Technical compliance has been re-assessed in line with the FATF Recommendations where: (i) the country has made legal, regulatory or operational framework changes since its last mutual evaluation or follow-up report with technical compliance re-ratings and (ii) there has been a change in the FATF Standards for which the country has not previously been assessed. Where technical compliance has been reassessed, the relevant section is clearly indicated in the Technical Compliance Annex. Where a Recommendation has not been re-assessed, the previous assessment is included under a grey heading (see Annex A. Technical Compliance).

A glossary of key terms is available at the end of the report.

Citing reference:

FATF (2026), *Mutual Evaluation Report of Türkiye*, FATF, Paris, https://www.fatf-gafi.org/en/publications/Mutualevaluations/turkiye-mer-2026.html

© FATF/OECD 2026



Attribution 4.0 International (CC BY 4.0)

This work is made available under the Creative Commons Attribution 4.0 International licence. By using this work, you accept to be bound by the terms of this licence. For information about reproduction, distribution and translation please see the Terms, Conditions and Disclaimers published on the FATF public website. You must not use the FATF logo, visual identity or cover image without express permission or suggest the FATF endorses your use of the work. Any dispute arising under this licence shall be settled by arbitration in accordance with the Permanent Court of Arbitration (PCA) Arbitration Rules 2012. The seat of arbitration shall be Paris (France). The number of arbitrators shall be one.

Table of contents

Executive summary 3

Roadmap of key recommended actions (KRAs) 18

Preface 21

Introduction to money laundering and terrorist financing risks and context 23

1 Assessment of risks, co-ordination and policy setting 36

2 International co-operation 47

3 Financial sector and virtual asset supervision and preventive measures 69

4 Non-financial sector supervision and preventive measures 99

5 Transparency and beneficial ownership 112

6 Financial intelligence 133

7 Money laundering investigations and prosecutions 150

8 Asset recovery 165

9 Terrorist financing investigations and prosecutions 182

10 Terrorist financing preventive measures and financial sanctions 200

11 Proliferation financing financial sanctions 214

Annex A. Technical compliance 225

Annex B. Technical compliance shortcomings 331

Glossary of acronyms 334

Executive summary

1. This report provides a summary of the anti-money laundering and counter-terrorist financing and proliferation financing (AML/CFT/CPF) measures in place in Türkiye as at the end of the onsite visit 28th November 2025. It analyses the level of compliance with the FATF 40 Recommendations and the effectiveness of Türkiye's AML/CFT system and provides recommendations on how this system could be improved.

Key Findings

a) Türkiye identifies, assesses and understands its ML/TF risks to a large extent including through its national risk assessment (NRA) process (three NRAs conducted (including two more) since its previous Mutual Evaluation Report (MER)) and related Threat and Vulnerability Working Groups as well as dedicated case discussions which assist with understanding of ongoing and evolving trends. Working groups also serve for policy development and co-ordinated action. Domestic co-operation is strong in Türkiye with frequent and positive interaction between Türkiye's Financial Intelligence Unit (FIU), the Financial Crimes Investigation Board (MASAK), law enforcement agencies (LEAs) and other competent authorities. Türkiye needs to deepen its understanding of cross-border ML/TF risks, including ML/TF involving trade and smuggling and track outcomes of policy for continuous improvement and further ensure effectiveness of its AML/CFT strategy.

b) Türkiye has a sound legal and institutional framework for international co-operation and generally seeks and provides mutual legal assistance, extradition and other forms of co-operation broadly in line with its risk profile. Authorities provide generally good quality assistance and make effective use of formal and informal co-operation channels, including strong police-to-police co-operation, FIU exchanges, liaison officers and joint investigations, which support foreign and domestic investigations, prosecutions and asset recovery, particularly in higher-risk areas such as ML, terrorism and TF. Türkiye also actively seeks international co-operation and makes broad use of co-operation mechanisms, including for beneficial ownership information and operational support. However, moderate shortcomings remain, including delays in some complex MLA matters, the absence of a mechanism to assess the quality of assistance provided, infrequent follow-up on delayed outgoing requests, inconsistent use of international co-operation to pursue assets moved abroad and limited extradition outcomes, although there is no indication that requests are arbitrarily refused. International co-operation is therefore functioning effectively, with notable operational strengths, while improvements are needed in timeliness, follow-up and the more consistent pursuit of cross-border asset recovery.

c) Türkiye has established a comprehensive framework for the licensing of all financial institutions (FIs), while for Virtual Asset Service Providers (VASPs) a solid regulatory framework was still being implemented at the time of the onsite visit, and the assessment team could not assess the effectiveness of its framework in practice. Overall supervisors have a good understanding of ML/TF risks, although sectoral supervisors have a less developed understanding of underlying risks, which may affect effective AML/CFT supervision. FIs and VASPs have a generally strong understanding of the ML risks they are exposed to, while understanding of TF risks is more limited across sectors outside the banking sector. Overall, FIs and VASPs have a thorough

knowledge of their AML/CFT obligations; however, important deficiencies remain in their effective implementation. In particular, politically exposed person (PEP) identification and monitoring is only partially effective, and shortcomings continue to be identified in suspicious transaction reporting. Moreover, the low levels of TF-related suspicious transaction reports (STRs) across several higher-risk sectors suggest constraints in the detection and reporting of TF-related activity relative to risk exposure. Türkiye's supervisory activities have an overall positive impact on compliance by FIs and VASPs. Yet, a relatively high number of breaches continue to be identified through supervisory activities in certain sectors, notably exchange offices, as well as among money or values transfer services (MVTS) and VASPs. Türkiye has also not sufficiently demonstrated that the most serious or systemic breaches have been appropriately addressed with sanctions that are proportionate and dissuasive and the absence of publication of sanctions further undermines their dissuasiveness.

d) Türkiye has a licensing framework in place for all designated non-financial businesses and professions (DNFBPs) and follows a risk-based approach (RBA) for the supervision of DNFBPs, all high-risk entities in the highest risk sectors (dealers in precious metals and stones (DPMS), real estate agencies (REAs) and accountants) are supervised yearly and medium risk ones have been supervised at least once over a three-year period. Supervision of the other sectors (lawyers and notaries) is scarce and not in line with the risks posed by some entities in those sectors. Beyond the scope of customer due diligence (CDD) requirements, supervision is limited on other AML/CFT obligations for all DNFBPs and did not demonstrate a tangible impact on the sector overall compliance. DNFBPs' understanding of ML/TF risks remains limited, but entities generally understand their AML/CFT obligations. DNFBPs, in particular those that are part of international groups, implement some measures to comply with those obligations. Yet, there remain gaps in the reporting of suspicious transactions and the implementation of internal controls across the DNFBP sector.

e) Türkiye has a generally good and evolving understanding of ML/TF risks associated with domestic legal persons, supported by the NRA, Legal Persons Risk Assessments (LPRAs) and strong operational understanding, although this understanding is less developed regarding foreign-created legal persons with sufficient links and foreign legal arrangements, and is uneven across competent authorities and obliged entities. Türkiye has established important mitigating measures to reduce misuse of legal persons, including transparency controls through the Trade Registry and MERSiS, a multi-pronged framework for beneficial ownership (BO) information, controls over bearer shares and robust monitoring arrangements for associations and foundations. The multi-pronged framework and high levels of BO reporting are positive features, but major improvements are needed to ensure basic and beneficial ownership information is consistently accurate and up to date, particularly through more systematic and risk-based verification. While competent authorities generally have timely access to ownership information, use of the full range of information sources appears uneven in practice, with concentrated reliance on core registries. Türkiye has strengthened its sanctions framework and applies administrative measures actively, but enforcement remains more limited in higher-risk areas, including fraudulent companies, foreign-created legal persons and certain registry obligations, reducing the overall deterrent effect.

f) MASAK plays a central and effective role in the receipt, analysis, and dissemination of financial intelligence. MASAK's broad and direct access to more than 300 databases, including STRs, cross-border declarations, and disclosures, provides a robust information base for producing high-quality financial intelligence to support ML, associated predicate offences and TF investigations and prosecutions. MASAK received STRs mostly related to some high and medium

high risk predicate offences, but STRs on TF, drug trafficking and smuggling are very limited. MASAK generates balanced proactive and reactive disseminations and can identify and trace complex ML/TF schemes, including criminal networks and their financiers. MASAK analysed the numerous number of STRs through strategic analysis work and limited number through mandatory scoring process and used for ML, TF, and predicate offences operational analysis and examination. Competent authorities make systematic and effective use of MASAK's intelligence, which is consistently assessed as relevant, timely and of clear added value at an operational level. However, some delays in the production of these reports were identified, which were considered to slightly affect the timeliness of enforcement actions in certain cases. MASAK has elevated its organisational expertise and resources including a significant upgrade in its information technology (IT) systems, contributing to the prioritisation of STRs analysis at an entry level improving the effective allocation of resources when analysing the information being submitted by reporting entities and subsequent analysis. Strong formal and informal interagency co-operation mechanisms further enhance the effective use of financial intelligence and support disruption strategies in ML, predicate offences, and TF investigations.

g) Türkiye has an appropriate legal and operational framework to identify and investigate all types of ML offences, including through parallel financial investigations (PFIs), limiting stand-alone ML cases to illegal betting in most cases. Türkiye's competent authorities identify ML activities utilising a wide range of information and investigative tools. Specialised public prosecutors lead ML investigations with the support of LEAs and other relevant competent authorities (i.e., MASAK). Investigations are generally triggered by referrals from other competent authorities, LEA's operational work and information from foreign counterparts. Türkiye has demonstrated its ability to conduct complex ML investigations leading to operational outcomes such as the disruption of ML criminal networks by prioritising interagency and international co-operation through formal and informal channels. Although Türkiye has investigated, prosecuted and convicted a substantial number of ML and predicate offences, the country's contextual and material factors (i.e., size of the financial sector, geographical position as a transit hub, and the extent of cash-based and size of informal economy) impact the nature of its exposure to ML risks and require further operational efforts in high-risk areas other than fraud (i.e., professional ML, misuse of legal persons and cross-border movements). Türkiye nevertheless presents challenges in fully translating investigations into judicial outcomes which generates a backlog in the number of pending prosecutions (7 248 cases) and convictions (6 085), comprising to a less extent prosecution and conviction on complex ML that involved professionals (9%). Sentencing ranges are proportionate effective and generally dissuasive for natural persons. Given the absence of criminal liability for legal persons, Türkiye can only apply administrative sanctions, which have been used in a limited number of ML cases and appear disproportionate to the country's risk profile.

h) Türkiye prioritises asset recovery as a national and operational policy objective at the highest level. To guarantee that its asset recovery system is kept up-to-date, Türkiye periodically reviews its policies by incorporating operational findings, trends and international experiences. Türkiye has mechanisms in place to help authorities in the rapid identification and tracing of criminal property and property of corresponding value. Türkiye presents challenges when assets are located abroad representing a major shortcoming in the overall asset identification and tracing mechanism. Although Türkiye has substantially applied postponement of transactions (asset freezing as a preventive measure), the number of assets seized and confiscated remains modest. Türkiye has appropriate mechanisms in place to manage, and dispose seized and confiscated assets to preserve their value. Assets repatriation and international enforcement mechanisms

are applied to a limited extent. Türkiye has a solid legal framework for cross-border cash declaration and disclosures coupled with high-level technology to detect illegal movements of cash at all land and air check points. Despite these efforts, the limited number of cross-border seizures of cash and other goods is concerning given Türkiye's risk and context.

i) Türkiye's geographic location significantly elevates its TF risk, as its proximity to conflict-affected regions and its role as a regional financial, trade and logistics hub expose it to use as a transit, procurement and financing channel for terrorist networks. In response, Türkiye's competent authorities have developed and implemented robust CFT policies and operational mechanisms, which are integrated into and continuously inform national strategies based on operational outcomes. Türkiye presents strong and institutionalised capabilities to identify and investigate TF in relation to those terrorist organisations identified as TF threats in its NRA (FETÖ, PKK/KCK-PYD/YPG, ISIL, AQ), but challenges remain in identifying TF activity involving other terrorist organisations and networks identified through international sources and co-operation channels as relevant to its TF risk exposure.

   Competent authorities have a strong degree of specialisation on TF methods and techniques. Operational detection is further supported by PFI being mandatory in all terrorism-related investigations, extensive interagency and international information-sharing arrangements and integrated databases strengthening investigative workflows across all competent authorities. The combination of high level of expertise and sophisticated investigative tools has led Türkiye to investigate, prosecute and convict a substantial number of cases related to those organisations identified as TF threats in its NRA.

   Operational focus also covers a wide range of TF activities, including a combination of traditional and sophisticated TF methods but challenges remain in the identification and investigation of cases involving layered commercial activities, trade-based TF (TBTF) and the involvement of legal persons in such activities. Sentencing ranges are generally effective, dissuasive and proportionate for natural persons but the limited implementation of administrative sanctions to legal persons in the context of a TF criminal investigation remains a concern.

j) With its current framework, Türkiye has been able to implement TF related targeted financial sanctions (TFS) without delay to some extent yet not systematically. The process takes place on an average of 2.5 days due to the time required for the United Nations (UN) listing decision to be transposed into domestic law. Türkiye has made use of its TF TFS framework to a large extent to mitigate its TF risks, demonstrating its ability to target assets of individuals and entities related to terrorist organisations, including UN designated terrorist organisations. FIs and VASPs are generally aware of their TF TFS obligations and comply to a certain extent while DNFBPs have a lesser understanding and compliance with those obligations. Supervisory activities on TF TFS are conducted following a RBA.

k) Türkiye classified some associations as non-profit organisations (NPOs), and excluded foundations from this scope, on the basis of their financial materiality and exposure to TF risk which is not fully in line with the FATF's functional definition of NPOs. Türkiye's NPOs monitoring also covers ML which goes beyond the scope of the FATF Standards. However, in practice Türkiye's monitoring of NPOs follows an RBA and is mostly focused on their potential abuse for TF purposes. Even though Türkiye's framework also provides for measures applying to the entire sector that could potentially disrupt or discourage legitimate NPO activities, the assessment team did not receive evidence that those are resorted to in practice. In line with its risk profile,

Türkiye has also identified several NPOs being abused for TF purposes and has taken mitigating measures accordingly.

l) Türkiye's competent authorities have a framework in place that ensures good co-operation and co-ordination in the implementation of policies for operational purposes on combatting proliferation financing and the financing of weapons of mass destruction.

They have an overall good understanding of PF risks yet risks related to potential sanctions evasions via the misuse of legal persons, including foreign ones, are understood to a lesser extent and could hinder Türkiye's ability to deter PF risks to some extent. Türkiye has a mechanism to implement PF TFS which ensures application without delay to some extent and not in a consistent manner.

Türkiye has been applying PF related TFS on Democratic People's Republic of Korea (DPRK) and Iran since 2021 and has listed individuals and entities accordingly in line with relevant UNSCRs and the FATF Standards for the vast majority of the reporting period. However, as of the end of the onsite visit, individuals and entities listed in relation to UN Security Council Resolution (UNSCR) 1737 and successor resolutions were still listed in Türkiye within the scope of UNSCR 2231 which no longer provides for the implementation of TFS since the snapback mechanism to UNSCR 2231 entered into force on 27 September 2025. Reporting entities' level of understanding and compliance with their PF related TFS is generally low.

Ratings for effectiveness and technical compliance

	Effectiveness		Technical Compliance	
Risk mitigation through policy, co-ordination and co-operation				
Assessment of risk, co-ordination and policy setting	**IO.1**	Substantial	**R.1**	Compliant
			R.2	Compliant
International co-operation	**IO.2**	Substantial	**R.36**	Largely compliant
			R.37	Compliant
			R.38	Largely compliant
			R.39	Compliant
			R.40	Largely compliant
Cross-cutting requirements			**R.33**	Largely compliant
Prevention, detection and reporting of illicit funds across sectors				
Financial sector and virtual asset supervision and preventive measures	**IO.3**	Moderate	**R.9**	Compliant
			R.10	Largely compliant
			R.11	Compliant
			R.12	Compliant
			R.13	Compliant
			R.14	Compliant
			R.15	Largely compliant
			R.16	Largely compliant
			R.17	Compliant
			R.18	Largely compliant
			R.19	Largely compliant
			R.20	Compliant
			R.21	Compliant
			R.26	Compliant
			R.27	Largely compliant
Non-financial sector supervision and preventive measures	**IO.4**	Moderate	**R.22**	Largely compliant
			R.23	Largely compliant
			R.28	Largely compliant
Transparency and beneficial ownership	**IO.5**	Moderate	**R.24**	Largely compliant
			R.25	Largely compliant
Cross-cutting requirements			**R.34**	Largely compliant
			R.35	Largely compliant
Detection and disruption of threats, sanctions and deprivation of illicit funds				
Financial intelligence	**IO.6**	Substantial	**R.29**	Compliant
Money laundering investigations and prosecutions	**IO.7**	Moderate	**R.3**	Largely compliant
Asset recovery	**IO.8**	Moderate	**R.4**	Largely compliant
			R.32	Largely compliant
Terrorist financing investigations and prosecutions	**IO.9**	Moderate	**R.5**	Largely compliant
Terrorist financing preventive measures and financial sanctions	**IO.10**	Moderate	**R.6**	Largely compliant
			R.8	Partially compliant
Proliferation financing financial sanctions	**IO.11**	Moderate	**R.7**	Partially compliant
Cross-cutting requirements			**R.30**	Compliant
			R.31	Largely compliant

Note: Effectiveness ratings can be either a High-HE, Substantial-SE, Moderate-ME, or Low-LE, level of effectiveness. Technical compliance ratings can be either a Compliant-C, Largely compliant-LC, Partially compliant-PC or Non-compliant-NC. While the technical compliance findings can be relevant across the effectiveness immediate outcomes (for example, R.1 or R.40), the table above illustrates the main technical compliance findings specific to each effectiveness immediate outcome and cross-cutting requirements for each of the intermediate outcomes. For more detail on the relevant technical compliance requirements relevant to each effectiveness immediate outcome, see the relevant paragraph at the beginning of each chapter. See also paragraphs 53 and 54 of the FATF 2022 Methodology for links between effectiveness and technical compliance ratings.

Risks and general situation

2. As a regional trade and financial hub, Türkiye is exposed to significant domestic and international ML/TF risks especially in the banking, MVTS and VASP sectors. These include serious threats from illegal activities of criminal organisations, terrorist organisations and, to a lesser degree, foreign terrorist fighters (FTFs) seeking to exploit domestic and cross-border vulnerabilities. The key ML threats generating significant proceeds of crime are related to fraud, illegal betting and gambling, drug trafficking and smuggling. Highest ML/TF risks are related to activities involving the use of cash, banks, VASPs, MVTS, DPMS, REAs and the misuse of legal persons that could be facilitated by legal and accountancy professionals.

3. Türkiye faces terrorism threats from different types of terrorist organisations. The main terrorist threats faced and identified by Türkiye are the: (i) Fetullahist Terrorist Organisation (FETÖ); (ii) separatist Kurdistan Workers' Party and its factions (PKK/KCK-PYD/YPG); and (iii) the Revolutionary People's Liberation Party/Front (DHKP/C), as well as Islamic State in Iraq and the Levant (ISIL), Al-Qaida and its affiliates and other terrorist organisations. The nature of TF risks is greatly influenced by the country's geographical position and its proximity to conflict zones and external threats which create a favourable ecosystem for terrorist threats to abuse a wide variety of methods and sectors for TF purposes and linkages with organised crime which add further complexity to the TF threats faced by Türkiye.

Assessment of risk, co-ordination and policy setting (Chapter 1; IO.1, R.1, 2, 33 & 34)

4. Türkiye has a generally good understanding of its ML/TF risks, supported by a comprehensive and data-driven NRA process and continuous analytical work co-ordinated by MASAK. The assessment process is based on a common and well-resourced methodology that combines quantitative and qualitative data. This activity is sustained through the Threat and Vulnerability Working Groups, which include relevant competent authorities and private-sector representatives, to support the continuous integration of emerging trends within the risk framework. Certain high-risk channels are not yet fully captured, including those related to foreign linked ML schemes, unlicensed MVTS, professional facilitators and cross-border cash movement vulnerabilities.

5. Türkiye has no exemptions from the application of FATF Standards based on risk and has used an RBA to calibrate both simplified and enhanced measures.

6. Türkiye has an overarching National AML/CFT Strategy (2021-2025) which requires all agencies to align with the NRA findings as well as several related action plans with specific items and a separate CFT Strategy. There is generally robust co-operation among competent authorities, particularly between the MASAK and LEAs. Policies and activities of authorities are aligned with ML/TF risks and activities are well co-ordinated, including through Threat and Vulnerability working groups which equally serve as a space for discussing policy and specific cases and joint task forces.

International co-operation (Chapter 2; IO.2; R.36-40)

7. Türkiye has a sound legal and institutional framework for international co-operation, supported by bilateral and multilateral arrangements, reciprocity, judicial co-operation bureaux, secure case-management tools, specialised expertise and extensive liaison networks. International co-operation is particularly important given Türkiye's role as a regional trade, transit and financial hub and its exposure to cross-border ML/TF risks linked to offences such as drug trafficking, smuggling, fraud, tax evasion, illegal betting and gambling, misuse of legal persons and terrorism. Feedback from international counterparts regarding Türkiye's rendering of international co-operation is broadly positive.

8. Türkiye provides mutual legal assistance (MLA) and extradition constructively and is generally viewed by international partners as an active and reliable counterpart. The jurisdiction has demonstrated the capacity to provide evidence, financial information, testimony, seizure and confiscation assistance and to support foreign investigations, including asset recovery.

9. Türkiye actively seeks international co-operation and issues a high volume of outgoing MLA and extradition requests, broadly in line with its risk profile. Türkiye also makes strong use of police-to-police, FIU, supervisory, customs and tax co-operation channels, including through liaison officers, MASAK, INTERPOL, Europol, Egmont, CARIN, World Customs Organization (WCO) and other regional platforms. These mechanisms have supported complex investigations, asset tracing, foreign predicate ML cases, BO information exchanges and asset restraint. Specialised expertise and prioritisation mechanisms, amongst other factors, also contribute towards timely and meaningful outcomes.

10. Moderate improvements are however needed to Türkiye's international co-operation framework. While incoming MLA is generally provided constructively, delays arise in some complex ML cases and the use of structured mechanisms to assess the quality of assistance provided could be strengthened. While Türkiye actively seeks international co-operation, follow-up on delayed outgoing requests is not always systematic and international co-operation is not used consistently to pursue assets moved abroad.

Financial sector and virtual asset supervision and preventive measures (Chapter 3; IO.3, R.9-21, 26, 27, 34 & 35)

11. Türkiye has established a comprehensive framework for the licensing of all FIs. MASAK, as the main AML/CFT supervisor, and sectoral supervisors access a wide range of information to perform effective market entry controls to prevent criminals and their associates from entering the market. Authorities also conduct checks after the license has been granted as part of their supervisory activities. For VASPs, a solid regulatory framework has recently come into force but is still being implemented and had not yet become fully applicable to the existing VASP population. Competent authorities demonstrated the ability to detect unlicensed actors and the diverse methods employed to conduct their unlawful activities, supported by inter-agency co-operation and information exchange. However, the identification of unlicensed MVTS activities remains challenging in practice, particularly where these activities are carried out alongside other licensed operations.

12. Overall, supervisors have a good understanding of ML/TF risks both at sectoral and entities level for FIs and VASPs. MASAK, as the main and primary AML/CFT supervisor, demonstrates strong AML/CFT expertise across different financial sectors, types of institutions and emerging threats. Sectoral supervisors demonstrate a less developed ML/TF risk understanding, with a greater focus on risk mitigation measures and, to a lesser extent, on the underlying and actual ML/TF risks themselves. Capital Market Board's (CMB) understanding of VASP-related ML/TF risks, as sectoral supervisor is still developing, in particular with regard to the technical specificities of VASP operations and the emerging risk profiles.

13. FIs and VASPs have a generally strong understanding of the ML risks they are exposed to and the main ML risks identified by FIs and VASPs are generally in line with the findings of the NRA. Understanding of TF risks is more uneven. While banks - representing more than 75% of the sector - demonstrated a good understanding of TF risks, other FIs and VASPs have a more limited understanding, mainly considering TF risks in the scope of TFS. Overall, FIs and VASPs have a thorough knowledge of their AML/CFT obligations. Reporting entities apply mitigating measures, in particular CDD and take measures to identify beneficial owners. General reporting of suspicion from the highest risk sectors (banking, MVTS and VASPs) is substantial, while it is low for other FIs. Yet there is an overall limited number of TF STRs across all sectors, in particular for exchange offices, MVTS, and VASPs. PEP identification and monitoring is only partially

effective, particularly among the largest group of exchange offices, which suggests constraints in TF detection and reporting relative to their assessed risk exposure.

14. The adoption of the risk-based supervision approach in 2020 has led to a significant increase in the number of AML/CFT compliance supervisions, including both off-site and on-site supervisory actions, particularly on high-risk entities. Türkiye's supervisory activities have an overall positive impact on compliance by FIs and VASPs. There is close and continuous communication between MASAK, sectoral supervisors and reporting entities, through frequent meetings, guidance documents, best practice papers and other ML/TF outreach efforts.

15. Overall, enhanced supervisory actions have contributed to improved implementation of preventive obligations and greater awareness of AML/CFT requirements among FIs and VASPs. At the same time a relatively high number of breaches continue to be identified through supervisory activities in certain sectors, notably exchange offices, as well as among MVTS and VASPs. Türkiye has also not sufficiently demonstrated that the most serious or systemic breaches have been appropriately addressed with sanctions that are proportionate and dissuasive. In addition, the absence of publication of AML/CFT sanctions and remedial measures further undermines their dissuasiveness and limits their preventive and deterrent effect across the FI and VASP sectors.

16. Enforcement actions are largely driven by the number of individual CDD and STR deficiencies identified during onsite inspections, reflecting the legal design of the sanctioning framework under which administrative fines are imposed on a per-breach basis through fixed statutory amounts, with a mandatory transaction-based minimum threshold applying to certain categories of FIs. By contrast, even serious and extensive structural deficiencies — such as inadequate internal oversight and control, risk-management frameworks or the absence of institution-wide ML/TF risk assessments — are addressed through supervisory action that relies, in the first instance, on written warnings and a grace period for remediation. The sanctioning framework is formally graduated; however, as escalation is conditional on non-remediation and such deficiencies are typically remedied at the warning stage, they do not, in practice, lead to escalation to punitive sanctions in the absence of concurrent individual CDD or STR breaches. As a consequence, these systemic weaknesses — although often more serious in nature than individual CDD-/STR-related breaches — are not met with sanctions that are proportionate to their severity or sufficiently dissuasive.

Non-financial sector supervision and preventive measures (Chapter 4; IO.4, R.22, 23, 28, 34 & 35)

17. Türkiye covers all non-financial sectors required to be covered for AML/CFT obligations by the FATF Standards (DNFBPs). Türkiye has a licensing framework in place for all DNFBPs and conducts fit and proper checks to a certain extent. The process is robust for accountants, lawyers and notaries. While authorities also perform fit and proper requirements for DPMS and REAs, those do not extend to associates of criminals. Türkiye detects unlicensed activities, in relation to DNFBPs, to some extent but the persistence of a high number of unlicensed actors in the REA and DPMS sectors remain a concern.

18. Türkiye has identified ML/TF risks across DNFBP sectors through a comprehensive risk assessment. Despite some positive steps taken by competent authorities, DNFBPs' understanding of ML/TF risks remains limited. In the DPMS and REAs sectors, the understanding of ML risks is more developed, especially for larger entities, while TF risk understanding is limited to awareness of TF related TFS obligations. Accountants, lawyers and notaries have a more limited understanding of ML/TF risks.

19. Larger DNFBPs, particularly those that are part of international groups, generally understand their AML/CFT obligations and implement measures to comply with them. While larger DNFBPs apply internal controls as a group policy, there is a lack of such measures in smaller DNFBPs across all sectors. Except for

DPMS, other DNFBP sectors barely report suspicious transactions, which is not in line with the risks they are exposed to, especially for REAs and accountants.

20. Türkiye follows a risk-based approach for the supervision of DNFBPs, all high-risk entities in the highest risk sectors (DPMS, REAs and accountants) are supervised yearly and medium risk ones have been supervised at least once over a three-year period. Nevertheless, supervision of the other sectors (lawyers and notaries) is scarce and not in line with the risks posed by some entities in those sectors. Beyond the scope of CDD requirements, supervision is limited to over AML/CFT obligations for all DNFBPs and did not demonstrate a tangible impact on the sector's overall compliance.

Transparency and beneficial ownership (Chapter 5; IO.5, R.24 & 25)

21. Türkiye has identified and assessed the main ML risks associated with domestic legal persons, supported by successive risk assessments and operational understanding, particularly regarding the misuse of companies in complex laundering schemes. Legal persons are recognised as an important vulnerability in the country's risk context, including in relation to trade-based activity, cross-border flows and more complex ownership structures. However, understanding of risks associated with foreign-created legal persons with sufficient links and foreign legal arrangements is less developed and not yet consistently reflected across competent authorities or obliged entities, particularly for TF risks and more complex cross-border structures.

22. Türkiye has implemented a broad framework to promote transparency and mitigate misuse, including company registration controls, a BO registry, controls on bearer shares, the non-recognition of nominee arrangements and mechanisms to address dormant companies. The multi-pronged framework for BO information, combined with complementary information held by registries, obliged entities and competent authorities, provides an important foundation for transparency and innovative features such as dematerialised bearer shares and structured monitoring systems for associations and foundations are recognised strengths. However, important weaknesses remain in ensuring that basic and BO information is consistently accurate and up to date, particularly due to reliance on self-reported information, limited substantive verification and uneven use of the full range of information sources available.

23. Competent authorities generally have timely access to ownership information, particularly for law enforcement purposes, but the use of BO information by non-law-enforcement authorities is less developed in practice. Measures to prevent misuse of higher-risk legal persons, including foreign-created legal persons with sufficient links, do not yet fully align with the country's risk profile. While the sanctions framework has been strengthened and active enforcement contributes to high formal compliance, enforcement remains less developed in higher-risk areas, including fraudulent companies and certain registry-related breaches and sanctions do not always appear sufficiently dissuasive in more complex ML/TF scenarios.

24. Türkiye's framework has materially improved transparency and reduces opportunities for anonymity, but major improvements are required particularly in the depth of risk understanding relating to foreign-linked structures, the verification of ownership information and the effectiveness and deterrent impact of preventive and enforcement measures.

Financial intelligence (Chapter 6; IO.6, R.29-32)

25. Türkiye's institutional and operational framework for the production and use of financial intelligence demonstrates strong and substantial results, particularly in relation to its highest ML/TF risks. MASAK, serves as the central authority for receiving, analysing, and disseminating STRs. MASAK received

STRs mostly related to some high and medium high risks predicate offences, but STRs on TF, drug trafficking and smuggling are very limited.

26. MASAK's broad and direct access to multiple sources of information provides a robust data base that enables the production of high-quality quantitative and qualitative financial intelligence and underpins its role as the main authority to produce financial intelligence. This is considered a major strength as it enables extensive real-time cross-checking and verification of data, significantly enhancing accuracy and reliability of the information when producing financial intelligence. Other competent authorities access financial and non-financial information through their own databases and can obtain additional data from MASAK, where needed, to support investigations and intelligence. MASAK analysed the numerous number of STRs through strategic analysis work and limited number through mandatory scoring process and used for ML, TF, and predicate offences operational analysis and examination.

27. Türkiye has a robust system for producing high-quality financial intelligence and other relevant information to effectively support competent authorities in ML, associated predicate offences, and TF investigations and prosecutions. MASAK relies on multiple IT tools, which enable the integration and analysis of data from across Türkiye's databases and support the production of comprehensive intelligence reports disseminated to relevant competent authorities. However, some delays in the production of these reports were identified, which were considered to slightly affect the timeliness of enforcement actions in certain cases. Competent authorities systematically acknowledge the substantial added value of MASAK's financial analysis to their operational work, widely using MASAK's financial intelligence products and other relevant information not only to pursue ML, associate predicate offences and TF investigations and prosecutions but also to trace assets.

28. Türkiye's competent authorities have close formal and informal co-operation mechanisms in place to exchange financial intelligence and other relevant information to pursue ML/TF investigations and prosecutions. Interagency co-operation mechanisms between MASAK and other competent authorities are solid and fluid, and, together with well-established international co-operation channels (including Egmont, joint investigations, and diagonal co-operation), have delivered positive operational results. These exchanges are supported by high-level confidentiality safeguards and secure, encrypted communication systems.

29. Overall, STRs and MASAK's financial analysis have effectively contributed to the initiation of significant ML, associated predicate offences, and TF investigations, as well as to the disruption of complex ML and TF schemes. MASAK's analysis is consistently recognised as a critical operational input, both when proactively disseminated to trigger potential cases and when provided in response to requests from operational authorities.

Money laundering investigations and prosecutions (Chapter 7; IO.7, R. 3, 30 & 31)

30. Türkiye has a robust institutional and well-resourced framework to investigate ML and predicate offences. Public prosecutors lead ML investigations which are supported by all LEAs, and when the specificity of the case needs it, they can request MASAK's experts' and other competent authorities for further analysis.

31. Türkiye identifies and investigates a broad range of ML activities, including through the systematic use of PFIs. Investigations are most commonly triggered by typologies such as cash deposits into bank accounts, the use of MVTS (licensed and unlicensed), VASPs, and money mules. While ML layering activities are investigated to a lesser extent, identified typologies include the creation of multiple small businesses and companies, professional laundering involving lawyers and accountants, and TBML. In most cases, integration is primarily achieved through investments in real estate and gold, as well as the establishment of small businesses and enterprises. Overall, Türkiye presented a substantial number of ML investigations

covering a wide range of schemes, although challenges remain in effectively addressing more complex laundering techniques, such as cross-border movement of currency, layered legal persons schemes and trade-related offences.

32. Türkiye extensively pursues prosecutions and recorded convictions related to all types of ML offences. Standalone ML prosecutions are only limited to illegal betting-related cases and has not been applied to other types of predicate offences. There are several case studies demonstrating the prosecution of foreign predicate offences triggered by domestic investigations which include foreign elements. Although ML prosecutions and convictions are in line with Türkiye's risk profile, particularly for fraud and illegal betting, this is not the case to medium-high risk and medium predicate offences (i.e., drug trafficking and smuggling). Prosecutors presented challenges in prosecuting complex ML schemes involving sophisticated layering structures, including legal persons, shell companies, misuse of legal professionals and trade-based mechanisms, and systemic layering networks, as well as the misuse of technology.

33. Türkiye imposes an average of 4-years 4 months imprisonment for natural persons convicted of ML charges which is considered effective, proportionate and dissuasive in general. The limited application of criminal sanctions in complex ML cases, particularly those involving professional money launderers and organised crime, weakens the overall dissuasive effect of the sanction's framework. In addition, while Türkiye has applied administrative sanctions to legal persons, the scale of these sanctions is neither sufficiently dissuasive nor commensurate with the country's ML risk profile. Türkiye also applies alternative measures when securing a ML conviction is not feasible, provided evidentiary standards are met (e.g., pursuing tax evasion or other predicate offences).

34. Overall, Türkiye has consistently raised the volume of ML investigations, prosecutions, and convictions, demonstrating an active enforcement response. However, persistent gaps in the identification, investigation and prosecution of high-risk predicate offences other than fraud (i.e., drug trafficking, smuggling and illegal betting), complex ML schemes (including, professional ML cases, organised crime and legal persons) and the application of disproportionate sanctions in these cases, limit the overall effectiveness of efforts to fully disrupt sophisticated ML networks and structures.

Asset recovery (Chapter 8; IO.8, R. 1, 4 & 32)

35. Türkiye prioritises asset recovery as a high-level national and operational policy objective. This long-standing focus is supported by regular updates to the legal framework and operational practices to reflect emerging risks, evolving typologies, and international standards. These policy efforts have progressively translated into concrete and measurable operational results.

36. The Coordination Board for Combating Financial Crimes (CBCFC) plays a central role in ensuring co-operation and co-ordination among all AML/CFT relevant competent authorities including in the development of strategies and mechanisms to enhance the effectiveness of asset recovery efforts, reviewing draft legislation and strengthening interagency co-operation when implementing asset recovery strategies.

37. Türkiye also demonstrates a good number of resources to prioritise asset recovery at an operational level and can identify and trace criminal property domestically, but challenges remain on the use of these tools to identify and trace assets located abroad. Considering Türkiye's risk and context profile, characterised by a significant trade activity, substantial foreign investments, exposure to smuggling risks and the presence of cross-border criminal organisations, the limited ability to identify and trace assets located abroad represents a major shortcoming that constraints the overall effectives of the country's asset recovery system.

38. Türkiye has made extensive use of postponement of transactions as a provisional measure equivalent to asset freezing, applying it to approximately EUR 1.138 M across a wide range of financial activities, including those involving VASPs. These measures can also be applied in the context of PFIs, and Türkiye has progressively deployed the full range of available asset recovery tools. Only a limited proportion of assets subject to postponement, lead to seizure or confiscation and ultimately result in permanent deprivation. This low conversion rate is not commensurate with Türkiye's risk profile and indicates deficiencies at later stages of the asset recovery process.

39. Competent authorities are not able to distinguish whether the assets subject to any of these measures are related to criminal property or property of corresponding value, which further limits the assessment on the extent to which asset recovery measures target all types of illicit proceeds in the context of a criminal investigation. Türkiye has mechanisms in place to manage and dispose of frozen and seized property to preserve its value.

40. In principle confiscation revenues cannot be allocated directly for the compensation of victims and these revenues need to integrate into the government general budget. However, there are four exceptions to this rule where victims can be compensated for their losses: remorse provisions, alternative sanctions applied to the criminal, settlements and civil lawsuits. Türkiye has returned a large number of assets/funds subject to seizure and/or confiscation to identified victims (EUR 151 M). Most of the returned assets relate to fraud and forgery (92%), followed by drug trafficking (3.6%) and theft (3.1%) cases.

41. Türkiye operates a hybrid system combining cash declaration and disclosure mechanisms for addressing non-declared or falsely declared cross-border movements of currency and bearer negotiable instruments (BNIs). Despite efforts to strengthen Customs Enforcement (CE) capacities and deploy advanced technologies in line with its International Co-operation Review Group (ICRG) Action Plan, the detection and seizure of such movements continue to remain limited.

Terrorist financing investigations and prosecutions (Chapter 9; IO.9, R. 5, 30, 31 & 39)

42. Türkiye's geographic location significantly elevates its TF risk, as its proximity to conflict affected regions and its role as a regional financial, trade, and logistics hub expose it to use as a transit, procurement, and financing channel for terrorist networks. Türkiye is also exposed to TF risks arising from terrorist organisations and networks not subject to designation under the United Nations Security Council (UNSC) or Türkiye's domestic regime but identified through international sources and co-operation channels as relevant to its TF risk exposure.

43. Türkiye identifies TF activity through different operational tools, including (i) broader terrorism investigations; (ii) domestic operational detection channels; (iii) foreign intelligence sharing or co-operation requests; and (iv) detection of positive matches when screening against sanctions lists. Turkish authorities also conduct PFIs in all terrorism-related cases. Türkiye has well-developed and institutionalised capabilities to identify and investigate TF for risks related to terrorist organisations, associated individuals, groups, undertakings and entities designated by the UNSC and those designated under Türkiye's domestic regime. Türkiye's operational focus covers a wide range of TF activities, which has led to the identification of TF schemes using a combination of traditional and sophisticated TF methods to raise, move, store and spend assets, which aligns with the TF threats identified in its NRA (FETÖ, PKK/KCK-PYD/YPG, ISIL, AQ).

44. The scale of investigations is significant, including over 11 000 TF investigations and broadly reflects Türkiye's high exposure to TF risks, which involve the potential misuse of a wide range of financial and non-financial sectors. Türkiye has implemented a holistic approach to identify the role of a terrorist financier in TF investigations, using different techniques to create a detailed financial footprint by

connecting financial traces with operational realities to accurately identify and attribute the financier's role. However, investigations focus primarily on the movement of funds, without fully demonstrating the final use, hierarchical roles, facilitators abroad, or the upstream organisational structure.

45. Türkiye has doubled TF prosecutions and substantially increased TF convictions since its previous MER (2019). While these efforts are greatly recognised, case studies and statistics point to uneven outcomes across the full TF risk profile, in particular, in relation to TBTF, procurement networks, complex legal person structures, foreign-created legal persons and foreign legal arrangements, and TF activity linked to other relevant organisations that are neither designated by the UNSC or Türkiye's domestic sanctions regime.

46. Türkiye has a robust sanctioning framework for natural persons convicted of TF, with imprisonment of 5-10 years for TF and 10-30 years when linked to organisational leadership, which is considered effective, proportionate and dissuasive. Administrative sanctions imposed to legal persons in relation to a TF offence are not effective, proportionate or dissuasive.

47. Türkiye has a well-developed domestic CT/CFT strategy, with structured inter-agency mechanisms and policy documents. TF investigation outputs are embedded in domestic CT/CFT strategies, supported by interagency co-ordination (e.g., Threat Working Group) and data integration into the NRA. The findings derived from investigations, prosecutions, and sentencing in TF-related cases constitute an important foundation for shaping Türkiye's TF and broader CT strategies and action plans.

48. Türkiye applies a range of alternative criminal justice and administrative measures in cases where securing a TF conviction is not practicable. While this provides an additional avenue to address unlawful conduct, the available information does not clearly distinguish between preventive and alternative measures, nor does it sufficiently demonstrate their contribution to disrupting the financial aspects of TF activity.

49. Overall, despite Türkiye's efforts in significantly increasing TF investigations, prosecutions and convictions since the previous MER in relation to UNSCR-listed and domestically designated terrorist organisations, a significant effectiveness gap remains in relation to terrorist organisations and networks that are not designated under UNSCRs or Türkiye's domestic regime but are identified through international sources and co-operation channels as relevant to Türkiye's TF risk exposure. This materially limits effectiveness, as it constrains Türkiye's demonstrated ability to identify and pursue TF activity across the full spectrum of its relevant TF risk environment.

Terrorist financing preventive measures and financial sanctions (Chapter 10; IO.10, R. 1, 4, 6 & 8)

50. With its current framework Türkiye has been able to implement TF related TFS without delay to some extent yet not systematically. The process takes place on an average of 2.5 days due to the time required for the UN listing decision to be transposed into domestic law. Turkish authorities can apply mitigating measures to address to some extent the potential delay with regard to domestic transposition. Türkiye proposed individuals to the 1267/1989 and 1988 Committees for designation, in line with its risk profile.

51. Türkiye has a robust framework and process for listing individuals and entities to its domestic designation (pursuant to UNSCR 1373) list and actively resorts to this tool. Türkiye has made use of its domestic regime and adopted asset freezing measures, including following requests from foreign countries in line with its risk profile. Türkiye has made use of its TF TFS framework to a large extent to mitigate its TF risks, demonstrating its ability to target assets of individuals and entities related to terrorist organisations, including UN designated terrorist organisations under both UNSCR 1267 and 1373 regimes.

52. FIs and VASPs are generally aware of their TF TFS obligations and complying to a certain extent while DNFBPs have a lesser understanding of those obligations. Supervisory activities are conducted following a risk-based approach. High and medium risks entities have been supervised on their compliance with TFS obligations except for legal professions and accountants. Reporting entities representing a medium to low risk, which account for the vast majority of entities within each sector, have been monitored to a much lesser extent.

53. Türkiye classified some associations as NPOs, and excluded foundations from this scope, on the basis of their financial materiality and exposure to TF risk which is not fully in line with the FATF functional definition of NPOs. Türkiye's NPOs monitoring also covers ML which goes beyond the scope of the FATF Standards. However, in practice Türkiye's monitoring of NPOs follows a risk-based approach and is mostly focused on their potential abuse for TF purposes. Even though Türkiye's framework also provides for measures applying to the entire sector that could potentially disrupt or discourage legitimate NPO activities, the assessment team did not receive evidence that those are resorted to in practice. In line with its risk profile, Türkiye has also identified several NPOs being abused for TF purposes and has taken mitigating measures accordingly.

Proliferation financing financial sanctions (Chapter 11; IO.11, R. 7)

54. Türkiye's competent authorities have a framework in place that ensures good co-operation and co-ordination in the implementation of policies for operational purposes on combatting proliferation financing (CPF) and the financing of weapons of mass destruction. They have an overall good understanding of PF risks supported by the recent publication of both a PF Strategy and NRA. Those documents also support the implementation of mitigating measures to some extent, but actions are still to be taken in light of their recent adoption. Risks related to potential sanctions evasions via the misuse of legal persons, including foreign ones, are understood to a lesser extent and could hinder Türkiye's ability to deter PF risks to some extent.

55. Türkiye has a mechanism to implement PF TFS. This mechanism is similar to the one implementing TF TFS which ensures application without delay, to some extent, however not in a consistent manner as the process takes place on an average of 2.5 days. Türkiye has been applying PF related TFS on DPRK and Iran since 2021 and has listed individuals and entities accordingly in line with relevant UNSCRs and the FATF Standards for the vast majority of the reporting period. However, as of the end of the onsite visit, individuals and entities listed in relation to UNSCR 1737 and successor resolutions were still listed in Türkiye within the scope of UNSCR 2231 which no longer provides for the implementation of TFS since the snapback mechanism to UNSCR 2231 entered into force on 27 September 2025.

56. Reporting entities' level of understanding and compliance with their PF related TFS is generally low. While banks comply with their obligations to a certain extent, there is a severe lack of understanding of PF risks in the other sectors, coupled with challenges on the concept of owner, which impede reporting entities' ability to identify methods of evading PF TFS beyond list screening.

Roadmap of key recommended actions (KRAs)

1. Türkiye underwent a Mutual Evaluation of its anti-money laundering / countering the financing of terrorism / countering proliferation financing (AML/CFT/CPF) measures in place during the onsite visit to the country from the 11th to the 28th of November 2025. This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the 2022 Methodology.

2. The MER identifies the strengths and weaknesses of Türkiye's AML/CFT/CPF system, including both the level of effectiveness and the level of technical compliance, and recommended actions for improvement. The highest priority measures are identified as Key Recommended Actions (KRA) and are included in this KRA Roadmap.

3. The following presents the KRA Roadmap for Türkiye as adopted by the FATF Plenary in June 2026. Based on Effectiveness and Technical Compliance Ratings, Türkiye is placed in enhanced follow-up. This KRA Roadmap also serves as the basis for Türkiye's follow-up process.

IO.3 (Financial sector supervision and preventive measures)

Türkiye should:

d) Enhance FIs' and VASPs' understanding of TF risks and related mitigating measures, in line with a risk-based approach, with particular focus on high and medium-high risk sectors, such as VASPs, exchange offices and MVTS.

e) Enhance compliance with AML/CFT obligations, including, *inter alia*, suspicious reporting (including TF related aspects where relevant) and PEP obligations, in FIs and VASPs, following a risk-based approach, and enhance compliance with CDD requirements in exchange offices.

f) Ensure that the sanctioning and supervisory enforcement framework, including the use of remedial measures, is applied in a manner that strengthens the preventive and deterrent effect of enforcement. In particular, ensure that sanctions applied in cases involving more severe or systemic breaches of AML/CFT requirements are proportionate and sufficiently dissuasive, in line with the risk-based approach, including through a clearer calibration of sanctioning decisions to the seriousness and systemic nature of the breaches.

IO.4 (Non-financial sector supervision and preventive measures)

g) Strengthen DNFBPs' understanding of ML/TF risks and of their related AML/CFT obligations.

h) Increase supervisory capacities for DNFBPs, this could be achieved either through strengthening MASAK's resources allocated to supervision and/or enhancing AML/CFT expertise and dedicated staff for sectoral supervisors.

i) Develop a comprehensive understanding of the ML/TF risks lawyers are exposed to and ensure that high risk entities in legal (lawyers and notaries) and accounting sectors are monitored regularly.

IO.5 (Transparency and beneficial ownership)

Türkiye should:

j) Enhance the understanding of ML/TF risks associated with foreign created legal persons with sufficient links, by refining the criteria used to define sufficient links on a risk basis, improving alignment between risk assessments and typology materials and developing a more differentiated understanding of TF risks across domestic and foreign-created legal persons, particularly in cross-border contexts.

k) Strengthen the use of the Trade Registry and MERSiS as active ML/TF mitigation tools throughout the lifecycle of legal persons, including at incorporation, to detect inconsistencies and enhance overall effectiveness while supporting risk management.

l) Prioritise more comprehensive, risk-based verification mechanisms to ensure that BO information is accurate and up to date. This may include strengthening verification of both the identity of the beneficial owner and whether the identified individual is in fact the true beneficial owner, alongside enhancing the filing and processing of discrepancy reports submitted by obliged entities and increasing the routine use of BO Registry data by competent authorities beyond law enforcement.

IO.7 (ML investigations and prosecutions)

Türkiye should:

m) Further prioritise ML investigations and prosecutions related to certain high-risk predicate offences (drug trafficking, smuggling and illegal betting) that involve complex ML cases, particularly linked to high-risk activities (professional ML, goods and cross-border movement of currency, misuse of legal persons).

n) Develop clear guidelines for ML prioritising prosecutions in line with Türkiye's risk profile with the aim of reducing the backlog of pending prosecutions.

o) Enhance the consistent application of sanctions against natural and legal persons convicted for ML to ensure they are effective and dissuasive, particularly in cases involving public officials in the criminal activity, professional money launderers and organised crime.

IO.8 (Asset recovery)

Türkiye should:

p) Strengthen its capacity to identify, trace and recover criminal assets located abroad, particularly in complex and cross-border criminal asset recovery cases. This requires both enhanced inter-agency co-ordination domestically and more systemic and timely use of international co-operation tools, including making a better use of MLA requests to recover these assets.

q) Strengthen cash controls effectiveness in customs supervised areas prioritising enhanced screening for inbound cash movements, including improved data analytics to identify high-risk patterns, increased co-ordination between Customs Enforcement, other LEAs and MASAK to ensure that declarations translate into enforcement outcomes.

IO.9 (Terrorist financing investigations and prosecutions)

Türkiye should:

r) Improve the identification, investigation and, where appropriate, the pursuit of prosecutions and convictions linked to the full range of TF threats aligned with their up-to-date risk profile. This should include operational guidance, case-handling standards and specialised training focused on risk-based identification of illicit activity beyond formally designated terrorist entities.

s) Further develop the identification, investigation and prosecution of complex TF cases, including trade-based TF, large-scale procurement networks and layered cross-border financial structures.

t) Strengthen the investigation and sanctioning of TF involving legal persons and commercial structures, including by increasing the use of security measures and administrative sanctions, to ensure broader and more consistent application beyond the FETÖ-related cases demonstrated.

IO.10 (Terrorist financing preventive measures and financial sanctions)

Türkiye should:

u) Ensure new designations for TF TFS are systematically implemented without delay.

v) Strengthen DNFBPs' understanding and compliance with TF TFS obligations.

w) Expand its supervisory efforts on TF TFS compliance for reporting entities, especially to those in sectors presenting high or medium risk of abuse for TFS purposes and that, within this category, have never been subject to a dedicated TFS supervision programme.

IO.11 (Proliferation financing financial sanctions)

Türkiye should:

x) Ensure it implements PF related TFS without delay.

y) Implement PF related TFS on Iran within the scope of UNSCR 1737 and its successor resolutions.

z) Strengthen reporting entities' understanding and compliance with PF related TFS.

Preface

This report summarises the anti-money laundering / countering the financing of terrorism / countering proliferation financing (AML/CFT/CPF) measures in place as at the date of the onsite visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT/CPF system and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the *2022 Methodology*[1]. The evaluation was based on information provided by the country, and information obtained by the Assessment Team during its onsite visit to the country from the 11th to the 28th of November 2025.

The evaluation was conducted by an Assessment Team consisting of:

- Ms. Jenna BEHRENDS, Public Prosecutor, Public Prosecutor's Office, Germany.
- Ms. Jonna EKSTRÖM, Chief Legal Advisor, Financial Supervisory Authority, Finland.
- Mr. 1st. Lieutenant Mohamed KHALED ALARAIFI, Financial Intelligence National Centre (FIU), Bahrain.
- Ms. Lakshmi KUMAR, Senior Policy Advisor, Africa-Western Hemisphere, Office of Global Affairs, Terrorist Financing and Financial Crimes, United States Treasury, United States.
- Mr. Alberto MENDOZA, Director of Supervision, Financial Information Unit (FIU), Argentina.
- Ms. Ferti Srikandi SUMANTHI, Senior Legal Analyst, Directorate of Law and Regulation, Indonesian Financial Transaction Reports and Analysis Centre (FIU), Indonesia.

with the support of the FATF and CFATF Secretariats: Ms. Diana FIRTH, Mr. Florent-Babacar DIENG, Ms. Sofia RAMIREZ (Policy Analysts) and Ms. Camille RENIE (Legal Advisor).

The report was reviewed by Mr. Carlos ACOSTA (International Monetary Fund), Mr. Jasper GIELKENS (The Netherlands) and Mr. Ian COLLINS (United Kingdom).

Türkiye previously underwent a Mutual Evaluation in 2019, conducted according to the *2013 FATF Methodology*. The 2019 evaluation, 2021, 2022 and 2023 follow-up reports have been published and are available at the FATF Website.

The 2019 Mutual Evaluation concluded that the country was compliant (C) with 11 Recommendations; largely compliant (LC) with 17; partially compliant (PC) with 10; and non-compliant (NC) with 2. As regards effectiveness, Türkiye was rated Substantial in IO.1 and IO.2; Moderate in IO.3, IO.4, IO.5, IO.6, IO.7, IO.8 and IO.9, and Low in IO.10 and IO.11.

Based on these results, Türkiye was placed in enhanced follow-up[2] and under ICRG review (successfully exiting this process in June 2024[3]). Since its last evaluation, Türkiye achieved the following re-ratings:

- One Recommendation upgraded from NC to C: R.12.
- Two Recommendations upgraded from PC to C: R.23 and R.26.

[1] The August 2024 Methodology was applied.

[2] For the purposes of the report, a country will be placed in enhanced follow-up if any one of the following applies: (a) it has 5 or more PC ratings for technical compliance; or (b) 1 or more NC ratings for technical compliance; or (c) it is rated PC on any one or more of R.3, R.5, R.6, R.10, R.11 and R.20; or (d) it has a moderate level of effectiveness for 6 or more of the 11 effectiveness outcomes; or (e) it has a low level of effectiveness for 1 or more of the 11 effectiveness outcomes.

[3] www.fatf-gafi.org

- Two Recommendations upgraded from NC to LC: R.7 and R.15 (R. 15 was rated PC in Türkiye's 1st FUR, after assessment against revised R.15 requirements then re-rated to LC).
- Eight Recommendations upgraded from PC to LC: R.6, R.8, R.18, R.22, R.24, R.25, R.28 and R.35.

In total, only one Recommendation (R.15) remained rated PC since the last evaluation of Türkiye. Türkiye remained in enhanced follow-up as of the start of its 5th round mutual evaluation in 2025.

Türkiye is now compliant or largely compliant with 38 out of 40 FATF Recommendations (only two partially compliant rated Recommendations remaining) and performing at a level of Moderate or Substantial levels of effectiveness in all eleven Immediate Outcomes.

Introduction to money laundering and terrorist financing risks and context

57. The Republic of Türkiye (referred to as Türkiye) is located between the continents of Asia and Europe, with a land area of 783 562 square kilometres. It has common borders with Armenia, Azerbaijan, Bulgaria, Georgia, Greece, Iran, Iraq and Syria. The country is a peninsula surrounded by the Black Sea, the Aegean Sea and the Mediterranean, and has maritime borders with the Republic of Cyprus[4], the Russian Federation, Ukraine and Romania.

58. Türkiye has a central government, based in the capital city Ankara, and administratively consists of 81 cities or provinces[5], geographically divided into seven regions. The official language is Turkish. The population of Türkiye is approximately 85.7 million (as of December 2024), and the largest city is Istanbul. The literacy rate is 96.8% (as of 2019), and life expectancy is 79 years for females and 72 years for males. The annual population growth rate is 0.24% since 2022.

59. Türkiye has a written constitution and a civil law system. Türkiye's hierarchy of laws comprises the Turkish Constitution (Constitution), international conventions, laws, presidential decrees, regulations and communiqués. Previous decrees and by-laws of the Council of Ministers are still in force, unless otherwise indicated in a new presidential decree or law. The Constitution is the highest legal document and no other legal instrument may contravene it. Legislative power belongs to the Grand National Assembly of Türkiye (GNAT) and the President, to some extent, in accordance with the Constitution.

60. Judicial power is vested in the high courts (Constitutional Court, Council of State, Court of Cassation and Court of Disputes) and lower courts. The Constitutional Court supervises the consistency and legality of laws, the Rules of Procedure of the GNAT and the decree laws relating to the Constitution. Its decisions are absolute, as published in the Official Gazette, and bind legislative, executive and judicial organs as well as administrative authorities, natural persons and legal persons. Türkiye is a party to the European Convention on Human Rights, and judgements of the European Court of Human Rights are binding in Türkiye.

[4] Note by Türkiye: The information in this document with reference to "Cyprus" relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Türkiye recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Türkiye shall preserve its position concerning the "Cyprus issue".
Note by all the European Union Member States of the OECD and the European Union: The Republic of Cyprus is recognised by all members of the United Nations with the exception of Türkiye. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

[5] In Türkiye, both "provinces" and "cities" are used interchangeably so the AT has also used both terms depending on the most appropriate context, in line with how Türkiye organises its agencies (e.g. for example "provinces" and "sub-provinces").

ML/TF/PF risks and scoping of higher-risk issues

Overview of ML/TF/PF risks

61. Türkiye faces significant ML and TF risks. These include serious threats from illegal activities of criminal organisations, terrorist organisations and, to a lesser degree, FTFs seeking to exploit domestic and cross-border vulnerabilities. The key ML threats generating significant proceeds of crime are related to fraud, illegal betting and gambling, drug trafficking and smuggling. Highest ML/TF risks are related to activities involving the use of cash, banks, VASPs, MVTS, DPMS, REAs and the misuse of legal persons that could be facilitated by legal and accountancy professionals.

62. Türkiye faces terrorism threats from different types of terrorist organisations, both domestic and international. Domestic threats can be ethnic, religious or ideologically motivated. The main domestic terrorist threats faced by Türkiye are: (i) FETÖ; (ii) PKK/KCK-PYD/YPG; and (iii) the DHKP/C.

63. As regards international threats, Türkiye is exposed to risks emanating from ISIL, Al-Qaida and its affiliates as well as other terrorist organisations. The nature of TF risks is greatly influenced by the country's geographical position and its proximity to conflict zones and external threats create a favourable ecosystem for terrorist threats to abuse a wide variety of methods and sectors for TF purposes, including the returning of FTFs. Linkages with organised crime add further complexity to the TF threats faced by Türkiye.

64. Türkiye faces PF risks to a lesser extent. These include exposure to PF risks through its trading routes and financial system that can be exploited to circumvent sanctions regimes. Türkiye shares borders with, and is a traditional trading partner of, Iran. Separately, Türkiye has limited diplomatic relations with DPRK.

Country's risk assessment and scoping of higher-risk issues

65. Türkiye has completed three NRAs since its previous FATF MER in 2019. Its 2023 and 2025 NRAs are based on a sound and well-developed Methodology which combines FATF's Guidance and Türkiye's own, self-developed Methodology including both quantitative and qualitative data with some adjustments in criteria between the 2023 and 2025 models to account for variations in risk. In 2025, Türkiye calculated the likelihood for both ML and TF based on 40 criteria/scenarios, including a likelihood, impact and vulnerability analysis for each threat element, as well as residual risk. Data analysed included case information from the national IT data collection and case management system (UYAP), from law enforcement agencies (LEAs), the Tax Inspection Board (TIB), international organisation reports, information from international co-operation/information exchange requests and open-source research. The NRA Methodology also considered the effect of mitigating measures in calculating residual risks and was supported by discussions within established Threat and Vulnerabilities Working Groups including both private and public sector and by experts' views (e.g. from MASAK Strategic Analysis, academia, etc.).

66. According to its 2025 NRA, Türkiye identified fraud, illegal betting and gambling, drug trafficking and theft and plundering as the main ML risks and the banking sector as the most abused in three out of those four offences, channelled through the banking, VASP, MVTS and REAs, depending on the offence.

67. In terms of scoping for increased focus, the Assessment Team (AT) prioritised measures to counter ML associated with fraud, illegal betting and gambling, as well as supervision and compliance of FIs, VASPs, and DNFBPs, particularly the DPMS and REA sectors, due to their materiality and the sectors growth since the 2019 mutual evaluation. The AT especially focused on the VASP sector, as a relatively new reporting entity in relation to more long standing, mature FIs (e.g. banks).

68. As Türkiye is exposed to high TF risk, the AT focused on Türkiye's understanding of the different methods used by domestic and UNSC-designated terrorist organisations (TOs) to raise, move, store and

spend funds or other assets, including proceeds from: illegal activities, mainly emanating from illegal taxation, smuggling (migrants, drugs, tobacco, commodity, fuel, historical artefacts, and weapons), movement of funds through unlicensed MVTS, virtual assets (VAs), crowdfunding and outward activities to finance TOs operating in other jurisdictions. The AT also considered how well the jurisdiction was identifying, investigating, prosecuting and convicting all types of TF activities and/or designating individuals as applicable, as well as tracing, seizing and confiscating assets, in line with its TF risk profile. The AT examined Türkiye's measures to prevent the abuse of non-profit organisations (NPOs) for TF purposes while ensuring their legitimate activity is not unduly disrupted or discouraged.

69. In terms of lower risk, the AT de-prioritised the insurance and casinos sectors as they were deemed less significant in terms of risk, context and materiality, with 88% of the insurance market dominated by non-life insurance premiums and casinos and non-state backed online gambling prohibited since 1998 and 2006 respectively.

Materiality

70. The official currency in Türkiye is the Turkish Lira (TRY)[6]. Türkiye has a gross domestic products (GDP) of United Stated Dollar (USD) 1 322 M and a GDP per person of USD 15 463[7]. Türkiye is considered the seventeenth largest economy in the world. Türkiye's major industries are: automotive chemical, construction, technology and electronics, food processing, furniture and decoration, iron, steel and metallurgy, textile and apparel and ready wear, packaging and logistics, defence, energy and natural resources, industrial machinery and white goods, gold and jewellery. Due to its geographical location and extension of its maritime borders, Türkiye is also considered a trading hub. In addition, given inter alia Türkiye's history as a central trade route between Europe and Asia, Istanbul is considered a regional financial centre providing direct access to world markets.

71. Germany, the United Kingdom, the United States, Iraq and Italy are the countries with the highest exports. The People's Republic of China (China), the Russian Federation, Germany, the United States and Italy are the countries with the highest imports. The real GDP growth rate was set at 4% for 2025 and expected to go up to 5% in 2027[8]. The inflation rate stood at 30% according to risk and context information provided by Türkiye.

Financial sector, VASPs and DNFBPs

72. For the purposes of this report, considering information provided by Türkiye and open sources, the banking sector is the most important sector in Türkiye, based on its materiality and ML/TF risk exposure, and is weighted as highly important. In terms of the total size of assets held in Türkiye, the banking sector is, by far, the biggest sub-sector of the Turkish financial sector. Banks constituted 80,67% and 75,65% of the financial sector in 2023 and 2024, respectively. The sector includes 34 deposit, 9 participation and 20 development and investment banks[9]. The banking sector is also recognised as the most abused both for ML and TF in the 2023 and 2025 NRAs, despite its maturity, high level of awareness and improvements in compliance.

73. The VASP sector, including 58 entities, is also given a high importance in terms of ML/TF risk due to its material presence in Türkiye. Türkiye is ranked 11th in the 2024 Global Crypto Adoption Index by

[6] The AT used the following conversion rate for EUR/USD values throughout the MER: RY to EUR (*0.20) and from USD to EUR (*0.86).

[7] Türkiye (2025), National Risk Assessment (NRA), Ministry of Treasury and Finance of the Republic of Türkiye, p. 35.

[8] NRA 2025, p.35.

[9] NRA 2025, p. 189.

Chainalysis and 14th in the same study in 2025[10]. Although VASPs were only recently required to be registered and licensed (in July 2024 and March 2025, respectively) they have been included as reporting entities since May 1st, 2021, and included in compliance supervision programs.

74. Exchange offices (EOs) are weighted as being moderately important, based on materiality and ML/TF risk exposure. A total of 773 exchange offices and 198 branches are active in Türkiye. The USD comprises the biggest share of EOs. In 2017, exchange transactions amounted to a total of USD 190 billion. In terms of the total size of assets held within Türkiye, the EO sector has 0.07% share of the overall financial sector[11] but cases have been noted of abuse of EOs by terrorist organisations which influenced their medium-high risk level.

75. The capital market sector has a 16.22% share of the Turkish financial sector and is the second biggest sub-sector behind the banking sector including 205 companies, 72 intermediaries, 69 portfolio management companies and 64 investment partnerships. The sector is weighted as moderately important.

76. Payment and electronic money institutions are also an important sector. There are 89 payment and electronic money institutions (PEMIs) in total, of which 26 are payment institutions (PIs) and 63 electronic money institutions (EMIs). The sector is risk assessed as medium-high including because of abuse for fraud, theft, robbery and corruption, and considering levels of compliance with AML/CFT obligations, the sector is weighted moderately important.

77. The Turkish insurance sector has a 5.34% share of the financial sector. 69 insurance and pension companies comprise the sector, including 49 non-life insurance companies and 20 life insurance companies. Of the total paid premiums, 88% are in non-life insurance and 12% of the total paid premiums are in life insurance.[12] There are 44 foreign-capital companies, of which 39 have a foreign capital share over 50%. Given relevant products, services, delivery channel and geographic risks, the sector is identified as medium-low risk in the NRA. The sector is weighted as being of a relatively lower importance than other sectors for the purposes of Türkiye's ME.

78. The non-bank financial sector represents 2.3% of Türkiye's financial institutions in terms of size of assets. A total of 124 companies are active in the sector, including 19 financial leasing companies, 24 financing companies, 48 factoring companies, 27 asset management companies and 6 savings and financing companies.[13] The ML/TF-related risk level is considered medium in the NRA (primarily because of STR reporting and compliance with AML/CFT obligations) and considered of moderate importance by the AT.

79. In the DNFBP sector, the precious metals and stones (jewellers) sector is considered as medium-high risk. According to the last Jewellery Sector Report prepared by the Ministry of Trade (MoT) in 2020, the sector produces approximately 300 tons of gold jewellery, placing Türkiye among the world's top ten jewellery-producing countries.[14] Gold mining in Türkiye in 2023 is estimated at USD 5.6 billion.[15]

80. ML risk in the real estate sector is also considered to be medium-high, because of the continued prevalence of real estate purchase being a dominant laundering method, despite no cases identified where real estate agents were directly facilitating the purchase, sales and/or rental transactions, and their

[10] NRA 2025, p. 236; Chainalysis (2025), *2025 Geography of Crypto Report*, https://www.chainalysis.com/wp-content/uploads/2025/10/the-2025-geography-of-crypto-report-release.pdf (accessed 8 December, 2025).

[11] NRA 2025, p. 40.

[12] NRA 2025, table 11.

[13] NRA 2025, P.199.

[14] NRA 2025, p. 222.

[15] Ministry of Energy and Natural Resources (available at: https://enerji.gov.tr/bilgimerkezi-tabikaynaklar-altin).

involvement not legally required for peer-to-peer transactions. The AT therefore attributed a relatively high weight to findings related to this sector.

81. The accountancy sector is highly regulated for matters other rather than AML/CFT, subject to registration and AML/CFT supervision. Therefore, the sector is assigned relatively less weight by the AT. The notary sector is assessed as low risk in Türkiye, due to several structural factors, including the professional profile of notaries, the AML/CFT obligations in place and the comprehensive and regular supervision they are subject to because of their notarial duties.

82. Lawyers can play a role in company formation and management, and in real estate transactions, although in practice they do not typically perform these functions in Türkiye. Lawyers were added as reporting entities in 2020 (following Türkiye's 2019 ME findings). The Constitutional Court annulled the relevant provision in January 2024 on the basis of concerns related to professional secrecy and filing STRs. However, the provision was restated in July 2024. These developments have influenced the sector's levels of compliance and risk profile to some extent, notwithstanding lawyers remain subject to AML/CFT obligations and supervision. The 2025 NRA assessed lawyers as medium-low ML/TF risk, and consequently, the AT gave the sector a moderate level of importance.

Table 1. Number of Obliged Financial Institutions and Asset Sizes

Institutions	Number of Institutions (Latest Data)	Period of the Latest Data	Asset Size (Latest Data) (Million TRY)	Asset Size (Latest Data) (Million EUR)	Share in the total asset size of the Financial Sector (%)	Period of the Latest Data
Banks	63	2024-12	32.657.234	1.959.434	75,65	2024-12
Financial Leasing Companies	19	2024-12	334.499	20.069,94	0,77	2024-12
Factoring Companies	48	2024-12	315.980	18.958,8	0,73	2024-12
Financing Companies	24	2024-12	212.542	12.752,52	0,49	2024-12
Asset Management Companies	27	2024-12	33.172	1.190,32	0,08	2024-12
Savings Finance Companies	6	2024-12	92.003	5.520,18	0,21	2024-12
Payment Institutions- Electronic Money Institutions	89	2014-12	110.185	6.611,1	0,26	2024-11
Intermediary Institutions	72	2024-12	252.083	15.124,98	0,58	2024-09
Portfolio Management Companies	69	2024-12	5.661.000	339.660	13,11	2024-12
Investment Partnerships	64	2024-12	1.087.414	65.244,84	2,52	2024-09
Non-Life Insurance Companies	49	2024-12	831.420	49.885,84	1,93	2024-12
Life Insurance and Pension Companies	20	2024-12	1.462.935	49.885,2	3,39	2024-12
Reinsurance Companies	4	2024-12	33.749	87.776,1	0,08	2024-12
Exchange Offices	773	2025-02	31.771[16]	1.906,26	0,07	2024-12

Precious Metals Intermediariy Institutions	46	2025-02	53.562[17]	3.213,72	0,12	2024-12
Total			43.169.549	2.590.173	100,00	

Note: conversion rates were calculated on reporting period (2020-2025) average (1 TRY=0.060), considering year 2020 (1 TRY=0.12 EUR); year 2021 (1 TRY= 0.097 EUR); year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); year 2024 (1 TRY= 0.028); and year 2025 (1 TRY= 0.022 EUR).
Source: Country submission

Table 2. Number of obliged institutions (DNFBPs)

Professional Group	Number	Regulatory Authority	Supervisory Authority
Jewellers	11.986	Min. Of Trade	Min. Of Trade and Professional Chambers
Real Estate Agents	77.831	Min. Of Trade	Min. Of Trade and Professional Chambers
Notaries Public	2.189	Min. Of Justice	Notaries Union of Türkiye, Min. Of Justice
Lawyers	199.142	Union of Turkish Bar Associations	Union of Turkish Bar Associations
Public Accountants, Certified Public Accountants and Sworn-in Certified Public Accountants	133.439	Min. Of Treasury and Finance	TÜRMOB and Min. Of Treasury and Finance

Source: Country submission.

Legal persons and arrangements

83. Legal persons in Türkiye are commercial companies that may take one of five forms: joint-stock companies, limited companies, general partnerships, commandite partnerships and co-operative companies. The establishment, basic features and functioning of these companies, with the exception of co-operatives, are regulated in the Turkish Code of Commerce (TCC, art.124). Co-operatives are regulated in Law No. 1163. MERSiS, which is the central registry system of the MoT, maintains a registry of relevant documentation for all commercial companies. Similarly, the KOOP-BIS system is used for co-operatives, VBYS for foundations and DERBIS for associations.

84. Joint stock company and limited company are the most common types of companies in Türkiye. Approximately 82.57% of all companies are limited companies, while 13.4% are joint stock companies and 3.4% are co-operatives. The number of legal persons registered according to their types is as follows:

Table 3. Distribution of Trading Companies in Türkiye

Type of Company	2020	2021	2022	2023	2024	2025
Joint Stock Company	142.249	158.097	178.091	197.976	215.098	223.915
Limited Company	859.570	958.218	1.083.805	1.204.586	1.314.337	1.388.132
Joint Ventures	1.083	1.210	1.372	1.627	1.864	2.108
Association Enterprise	2.707	2.799	2.916	3.016	3.047	3.098
Foundation Enterprise	962	957	978	990	1.002	981
Collective Company	10.876	10.732	10.667	11.145	11.106	11.047
Commandite	2.031	2.024	2.023	2.023	2.020	1.988
Co-operative	48.954	49.436	50.317	52.605	54.439	49.864
TOTAL	1.068.432	1.183.473	1.330.169	1.473.968	1.602.913	1.681.133

Source: *MERSIS*

85. Türkiye is not a company or trust formation centre. Turkish law does not recognise trusts and Türkiye is not a party to the Hague Convention.

Structural elements

86. Türkiye has the structural elements required for an effective AML/CFT/CPF system, including political and institutional stability and the rule of law, as embodied in its Constitution. Türkiye has also demonstrated high-level political commitment to address AML/CFT/CPF issues both during its ICRG review process which ended in June 2024 and its 5th ME process.

Background and other contextual factors

87. As of 2021, 74% of the Turkish population over the age of 15 was reported to have a bank account: Global Findex Database 2021 (World Bank)[18]. Türkiye has a well-developed AML/CFT/CPF legal and regulatory framework.

88. Despite the progress achieved and the enhancements made to the legal framework since 2020, including by adding specific analysis on foreign bribery in its 2025 NRA and several legislative amendments, Türkiye's foreign bribery enforcement framework continues to require further strengthening. In particular, reforms to the corporate liability legislation remain necessary, consistent with the Organisation for Economic Co-operation and Development (OECD) Working Group on Bribery in International Business Transactions. The OECD[19] remains concerned that Türkiye has still not enacted legislation to address long-standing recommendations, notably to reform its laws on the liability of legal persons for the bribery of foreign public officials. Türkiye's corporate liability framework does not clearly cover state-owned and state-controlled enterprises, and the prosecution or conviction of a natural person is a necessary basis for sanctioning legal persons. Furthermore, sanctions for legal persons are not sufficiently effective, proportionate and dissuasive.

AML/CFT/CPF strategy

89. Türkiye's AML/CFT work is guided by its "Strategy Document on Combating the Laundering of Proceeds of Crime and Financing of Terrorism and Increasing Effectiveness in Confiscation Practices in Türkiye (2021-2025)" (hereinafter referred to as the "AML/CFT Strategy"). Through 45 activities under 5 strategic objectives and 15 targets the document aims to improve the country's capacity to combat ML/TF. The five strategic objectives are 1) effective execution of judicial and administrative processes related to ML/TF, 2) ensuring that the NRA for combating ML/TF is up to date; 3) prioritising judicial and administrative processes involving financial aspects of ML/TF in line with assessment results, 4) assessing the legislative infrastructure and effectively implementing all judicial and administrative measures to seize and confiscate assets derived from crime in the context of the ML/TF and related predicate offences, and 5) conducting studies to ensure the effective use of targeted financial sanctions within the scope of combatting TF.

[18]World Bank, Global Findex 2021 Database, https://documents1.worldbank.org/curated/en/099818107072234182/pdf/IDU06a834fe908933040670a6560f44e3f4d35b7.pdf, page 26

[19] (OECD 2024), Implementing the OECD Anti-Bribery Convention Phase 4 Report of Türkiye, OECD Publishing, Paris, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/implementing-the-oecd-anti-bribery-convention-phase-4-report-turkiye_47986055/2db5c502-en.pdf, accessed 29 December, 2025).

90. The overall AML/CFT Strategy is underpinned by specific interrelated strategies and action plans such as the "Strategy Document on Combating the Financing of Terrorism" which determines Türkiye's priorities in combating TF and notes the need to combat all aspects of terrorism including TF, among the foremost security priorities of Türkiye.

91. Separately, work on CPF is guided by the Strategy Document on Increasing Effectiveness in Countering the Proliferation of Weapons of Mass Destruction (CPWMD) in Türkiye (2025-2029) which has the following four strategic objectives: 1) strengthening national co-ordination of CPF, 2) following international research and enhancing co-operation in CPF 3) developing supervision mechanisms to combat WMD (including CPF supervision) and 4) ensuring up-to-date NRA on PF and disseminating the NRA report.

92. There are also several interconnected strategies and action plans related to top predicate offences which affect the AML/CFT/CPF strategies such as work to combat smuggling and organised crime.

Legal and institutional framework

93. Türkiye's key AML/CFT/CPF legislation includes the following laws, regulations and communiqués amended and strengthened through the years, especially after Türkiye's 2019 ME, subsequent follow-up process and ICRG's review which ended in June 2024:

- Law No. 5549 (Prevention of Laundering Proceeds of Crime Law);
- Law No. 6415 (Prevention of the Financing of Terrorism);
- Law No. 7262 on the Prevention of Financing the Proliferation of Weapons of Mass Destruction
- Presidential Decree No. 1 on the Organisation of the Presidency;
- Regulation on Measures Regarding Prevention of Laundering the Proceeds of Crime and Financing of Terrorism (RoM);
- Regulation on the Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism (RoC);
- Regulation on the Procedures and Principles Regarding the Implementation of Law on the Prevention of the Financing of Terrorism (RoTF);
- Regulation on Principles and Procedures Regarding the Implementation of the Law on Prevention of the Financing of the Proliferation of Mass Destruction Weapons (RoPF); and
- MASAK regulatory instruments (i.e. General Communiqués).

94. The institutional framework for AML/CFT/CPF is broad, involving a range of ministries and authorities and has gone through significant change and reinforcement since Türkiye's 2019 Mutual Evaluation:

Ministries and co-ordinating bodies

- **Ministry of Treasury and Finance (MoTF):** The MoTF is responsible for preparing and implementing fiscal policies, managing public financial assets and liabilities, providing legal and revenue services to the government, fulfilling accounting operations and ensuring co-ordination amongst Türkiye's economic actors. Apart from MASAK, which operates as an independent unit housed within the MoTF, other primary units and departments within the MoTF are the TIB and General Directorate of Insurance (GDI), Insurance Supervision Board and Board of Treasury Comptrollers. Tax inspectors, Treasury controllers are also designated as examiners for ML examinations and supervision of obligations under the AML Law.

- **Financial Crimes Investigation Board (MASAK)**: MASAK[20] is the Turkish FIU and apart from its core responsibilities as an FIU, it also plays a central co-ordinating role in the Turkish AML/CFT system. Overall, MASAK is responsible for collecting STRs and other data, as well as analysing, evaluating and disseminating its findings to relevant authorities, including public prosecutors. MASAK is also tasked with developing policies and implementing strategies, preparing draft legislation and ensuring co-ordination amongst relevant bodies. Furthermore, MASAK is the supervisory body tasked with ensuring supervision of AML/CFT/CPF obligations by reporting entities.
- **Co-ordination Board for Combating Financial Crimes (CBCFC):** The CBCFC co-ordinates the activities of relevant institutions and establishments and determines the policies, practices, regulations and proposals for the prevention of ML/TF. The Board meets at least twice a year and comprises members from all government agencies, which have responsibilities for combating ML/TF.
- **Assessment Commission (AC):** Under the chairmanship of the Head of MASAK, the AC submits opinions and proposals to the Office of the Presidency relating to asset freezing requests (and their repeal) made by foreign countries, freezing requests (and their repeal) to foreign countries and also referrals to the Public Prosecutor's Office (PPO). The AC is the competent technical body for UNSCR 1373. Its decisions are non-binding, and MASAK provides secretariat services to the AC.
- **Ministry of Justice (MoJ):** The main responsibilities of the MoJ are establishing and organising the courts and other judiciary institutions, inspecting them with regard to their administrative duties, submitting suggestions to the Council of Judges and Prosecutors, maintaining criminal records, carrying out procedures related to foreign countries in matters of judicial services and evaluating draft bills. The primary units involved in the MoJ regarding AML/CFT efforts are the General Directorate of Legislation, the General Directorate of Foreign Relations and the European Union, the General Directorate of Penal Affairs and the General Directorate of Judicial Registration and Statistics.
- **Ministry of Interior (MoI):** The MoI exercises policy control over the General Directorate of Security (Turkish National Police), which is responsible for policing all crimes in urban areas; the General Command of Gendarmerie, which conducts policing in rural areas; and the Coast Guard, which is responsible for Türkiye's coasts. The MoI also prepares and implements regulations relating to law enforcement. Investigations are conducted under the authority of a public prosecutor. Several divisions within the MoI's departments are responsible for combating ML/TF.
- **Ministry of Foreign Affairs (MoFA):** The MoFA is involved in international co-operation, the negotiation of international agreements and approval of international conventions. The MoFA presents reports addressing Türkiye's implementation of counter-terrorism and counter-terrorist financing resolutions of the United Nations Security Council (UNSC). It co-ordinates with relevant units in Türkiye to evaluate requests received from other countries for co-operation and information exchange with regard to terrorism and TF. It also co-ordinates Türkiye's implementation of the UNSCRs related to proliferation financing**.**
- **Ministry of Trade (MoT)**: The MoTis responsible for the law relating to legal persons and arrangements and customs-related issues. It has a regulatory and audit role in relation to companies' activities with regard to the Trade Registry and in relation to the establishment of, and statutory changes in, commercial companies.

[20] The report will reference to MASAK and FIU indistinctively.

Supervisors/Regulators

- **MASAK:** As noted above and explained under supervisory arrangements further below, MASAK is the supervisory body tasked with ensuring supervision of AML/CFT obligations by reporting entities.
- **Directorate General of Foundations (Ministry of Culture and Tourism):** Duties of the Directorate include the supervision of foundations, research and development activities related to foundations and national and international co-ordination.
- **Central Bank of the Republic of Türkiye (CBRT):** The primary aim of the Central Bank is to achieve and maintain price stability. Its key duties include granting licenses to systems operators, which fall under the categories of Payment and Securities Settlement Systems and PEMIs; enhancing the stability in the financial system; taking regulatory measures with respect to money and foreign exchange markets; implementing regulations; supervising compliance with regulations and monitoring financial markets.
- **Banking Regulation and Supervision Agency (BRSA):** BRSA is responsible for regulation, monitoring and audit operations of all domestic and foreign banks operating in Türkiye, leasing companies, factoring companies, consumer finance companies, financial holding companies and asset management companies. BRSA is authorised to issue regulations and communiqués through Board decisions.
- **Capital Markets Board (CMB):** The CMB is the regulatory and supervisory authority in charge of the securities markets in Türkiye. The three primary areas within the responsibility of the CMB are: primary markets, secondary markets and financial intermediation. The CMB licences intermediary institutions and collective investment institutions, registers corporations issuing securities, and supervises clearing organisations as well as securities and precious metal exchanges established in Türkiye.
- **Insurance and Private Pension Regulation and Supervision Authority (IPRSA):** the IPRSA is the regulatory and supervisory authority in charge of the regulation, supervision and monitoring activities related to the insurance and private pension sectors.

Self-regulatory bodies

- **Banks Association of Türkiye (BAT):** Founded in 1958, is a public professional organisation that aims to contribute to the development of the banking sector and the banking profession.
- **Participation Banks Association of Türkiye:** It is a public professional organisation established in 2001 to ensure the development of participation banking operating in the field of Islamic finance.
- **Turkish Capital Markets Association:** It was established in 2001 as a public professional organisation representing the institutions authorised by the Capital Markets Law.
- **Insurance Association of Türkiye:** is a public professional organisation established in 1954 to ensure the development of the sector.
- **Association of Financial Institutions:** public professional organisation established in 2012 in accordance with the Law on Financial Leasing, Factoring, Financing and Savings Finance Companies.
- **Payment and Electronic Money Institutions Association of Türkiye:** public professional organisation established in 2019 within the framework of Law No. 6493 on payment and electronic money services
- **Association of Precious Metals, Stones and Foreign Exchange Market Institutions:** The Association of Precious Metals, Stones and Foreign Exchange Market Institutions, whose founding members are Borsa Istanbul A.Ş. Precious Metals Market intermediary institutions, is a voluntary association working on the development and the problems of the precious metals and stones market.

- **Association of Exchange Offices:** Association of Exchange Offices, which previously started its activities under the name of Exchange Offices Platform of Türkiye, commenced operating as a professional association on 23 October 2021, aiming to ensure unity for all exchange offices across the country and to take joint decisions.
- **Notaries Union of Türkiye:** Public professional organisation established in 1972. The main purpose of the Union is to protect the rights and interests of notaries, to continuously develop the notary profession and to ensure that it is a symbol of permanent trust.
- **Real Estate Agents Federation of Türkiye:** Real Estate Agents Federation of Türkiye was established in 2005 by Real Estate Professional organisations.
- **Union of Chambers of Certified Public Accountants:** Public professional organisation established in 1989 within the framework of the Law No. 3568 on Certified Public Accountants in order to carry out activities related to the development of the profession.
- **Chambers of Dealers of Precious Metals and Stones:** Professional organisations that aim to develop professional solidarity among their members and ensure standardisation in production and to keep records of daily market information.
- **Union of Turkish Bar Associations:** A professional organisation serving as an umbrella organisation established in 1969 with the participation of all bar associations in Türkiye.

Criminal justice and operational authorities

- **Public Prosecutors:** Public prosecutors are responsible for: i) conducting or enabling the conduct of criminal investigations, including those related to ML, predicate offences and TF, and to pursue asset recovery-related measures (seizure and confiscation); ii) monitoring and attending trial proceedings and applying for legal remedies, as necessary; iii) taking action to execute court decisions; and iv) exercising other duties assigned, in accordance with the law. Public prosecution offices are set up in each province or sub-province in which a court exists (Article 16 of Law No. 5235). PPOs are present in all 81 provinces and act independently. Each PPO is directed by the Chief Public Prosecutor.
- **Turkish National Police (TNP):** The General Directorate of Security or the TNP is a state organisation responsible for internal security, first established on 10 April 1845 and today organized in all provinces and districts in Türkiye.
- **Gendarmerie General Command (GGC):** The GGC of the Republic of Türkiye is an armed general law enforcement force that ensures security and public order and peace and fulfils the duties assigned by other laws and presidential decrees. The GGC is generally responsible for the areas that are outside those of police, i.e. places outside the provincial and district municipal borders or where there is no police organisation. However, places that are within the municipal borders may be determined as the gendarmerie's area of duty and responsibility when deemed appropriate in terms of service requirements. The general duties of the gendarmerie are as follows; to ensure, protect and safeguard security and public order, to prevent, pursue and investigate smuggling, to take and implement the necessary measures to prevent the commission of crimes, to guard the exteriors of prisons, to carry out the procedures specified in the laws regarding the crimes committed and to fulfil the judicial services related to them, to fulfil the military services given by laws and Presidential decrees.
    - **GGC– Department of Counter-Terrorism (TEM)**: The area of responsibility of GGC TEM is to carry out all kinds of operational activities and combats against terrorism, terrorists and terrorism financing and it is generally responsible for setting out and following the principles for Anti-Terrorist Operations, obtaining and evaluating terrorism intelligence, taking necessary measures to prevent and pursue crime, performing judicial law enforcement duties when necessary, organizing operations with the orders and instructions of judicial and civil authorities, reporting the detected crime and suspicion of crime to the judicial authorities,

carrying out investigation procedures when necessary and fulfilling the duties given during the prosecution phase, co-ordinating operational activities that cover more than one province and/or have an international dimension, collecting information and data and processing, classifying, analysing, evaluating and interpreting data, identifying the causes of major terrorist incidents by examining them, warning the relevant units about possible developments and measures to be taken in line with the orders of the General Command. It takes part in the activities of the Threat and Vulnerability Working Groups.

Preventive measures

95. Türkiye's preventive measures are set out primarily in the AML Law (Law No. 5549) and the TF Law (Law No. 6415), as well as four separate regulations as detailed further above in this report: the RoM, the RoC, the RoTF and the RoPF. Türkiye has not exempted specific sectors or activities from FATF requirements and has applied AML/CFT preventive measures to additional sectors in line with risks identified (e.g. lottery and betting, car dealers).

Supervisory arrangements

96. Türkiye supervises all sectors and activities covered under the FATF Standards. MASAK is the main AML/CFT/CPF supervisory authority in Türkiye. All FIs, DNFBPs and VASPs and other reporting entities are subject to AML/CFT/CPF supervision carried out by MASAK. In addition, BRSA, CMB, CBRT, IPRSA, and MoTF have AML/CFT licensing and supervisory roles in the financial and VASP sector.

Table 4. Financial institutions, VASPs, DNFBPs and their supervisors

Financial Institutions/VASP/DNFBPs	Licensing/Supervisory Authority
FIs and VASPs	
Banks, financial leasing companies, factoring companies, financing companies, asset management companies	BRSA
Payment institutions and e-money institutions	CBRT
Intermediary institutions, portfolio management companies, real estate investment companies, securities investment companies and private equity venture capital investment companies, VASPs	CMB
Life and non-life insurance companies, pension companies and re-insurance companies	IPRSA
Exchange offices Precious metals intermediary institutions	Ministry of Treasury and Finance (MoTF) General Directorate of Financial Markets and Foreign Exchange and Treasury Comptrollers Board (for supervision)
DNFBPs	
Casinos	Casinos are not allowed in Türkiye
TCSPs	There are no separate categories of TCSPs in Türkiye
Accountants	Supervisory Board of the Chambers of Accountants/ MoTF
Notaries	Union of Turkish Bar Associations/MoJ
Real Estate Agents	Ministry of Trade/Professional Chambers/Tax Inspection Board
Dealers in Precious Metals and Precious Stones	Ministry of Trade/Professional Chambers/Tax Inspection Board

International co-operation

97. Türkiye has a sound legal basis, including extensive memorandum of understanding (MoU) and bilateral and multilateral agreements as needed, to provide and seek the widest possible range of MLA, including extradition, in relation to ML cases, associated predicate offences and TF. Türkiye can also provide international co-operation on the basis of reciprocity. The central authority for co-ordinating MLA requests (including extradition) in Türkiye is the Directorate General for Foreign Relations and the European Union of the MoJ. Competent authorities such as MASAK, financial supervisors, LEAs, tax authorities and customs engage in other forms of international co-operation on the basis of laws and agreements.

98. Türkiye's major export/import countries are Germany and China respectively.

1 Assessment of risks, co-ordination and policy setting

The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this chapter are R.1, 2, 33 and 34 and elements of R.15.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Türkiye has a generally good understanding of its ML/TF risks, supported by a comprehensive and data-driven NRA process and continuous analytical work co-ordinated by MASAK. The assessment process is based on a common and well-resourced methodology that combines quantitative and qualitative data. This activity is sustained through the Threat and Vulnerability Working Groups, which include relevant competent authorities and private-sector representatives, to support the continuous integration of emerging trends within the risk framework. Certain high-risk channels are not yet fully captured, including those related to foreign linked ML schemes, unlicensed MVTS, professional facilitators and cross-border cash movement vulnerabilities.

b) Türkiye has an overarching National AML/CFT Strategy (2021-2025) which requires all agencies to align with the NRA findings as well as several related action plans with specific items. Türkiye also has a separate CFT Strategy with detailed actions to ensure that, among others, TF investigations and prosecutions are in line with Türkiye's risk profile. There is scope to further strengthen the extent to which strategic initiatives are translated into measurable outcomes across all risk areas.

c) Türkiye has a well-developed and operationally informed understanding of TF risks, supported by MASAK's analytical capabilities and access to a wide range of financial and non-financial information, including strong awareness of key threat actors, financing channels and sectoral vulnerabilities. However, the current actor-centric focus limits a more comprehensive understanding of how TF risks materialise across financial and non-financial systems, particularly in relation to non-designated actors, informal channels and cross-border activity.

d) The NRA process is complemented by additional assessments, including the LPRA and the NPO risk assessment, which provide further insights into sectoral vulnerabilities and misuse risks. However, risks associated with foreign-created legal persons and legal arrangements are not yet

fully articulated, particularly in terms of how they may be exploited in practice in cross-border contexts.

e) Türkiye demonstrates good awareness of sectoral risks, including high-risk areas such as real estate, banking, and payment systems, and has taken steps to address misuse across these sectors. However, in some cases—such as the real estate sector—the framework does not fully reflect how the market operates in practice, particularly where transactions occur outside regulated intermediaries, which may affect the effective application of AML/CFT measures.

f) Türkiye has no exemptions from the application of FATF Standards based on risk and has used an RBA to calibrate both simplified and enhanced measures. Policies and activities of authorities are aligned with ML/TF risks and activities are well co-ordinated, including through Threat and Vulnerability working groups which equally serve as a space for discussing policy and specific cases. Where needed, Türkiye also establishes joint task forces for specific cases. Some variation remains in how risk understanding is translated into supervisory and preventive outcomes, particularly in the consistent application of risk-based prioritisation across sectors and in ensuring that supervisory responses fully reflect the scale and nature of underlying risks.

g) There is generally robust co-operation among competent authorities, particularly between the MASAK and LEAs, supported by ongoing communication and structured engagement through working groups. This co-operation is also reflected in regular interactions with public prosecutors across provinces. While co-ordination mechanisms are well established and functioning effectively, there is scope to further strengthen the consistency of operational engagement across all relevant authorities, particularly in areas involving cross-border activity and systemic risks.

Recommended Actions

Türkiye should:

a) Strengthen its understanding of cross-border ML/TF risks, including of trade and smuggling. This could be achieved through collecting further quantitative and qualitative information on trade finance, shipping activity, customs controls, logistics and cargo operations and cross-border cash or value movements.

b) Adopt an AML/CFT strategy for the real estate sector in line with how the sector operates in practice, which includes a significant volume of direct buyer-seller dealings, to ensure that national policies and risk assessments are responsive to ML/TF risks already identified.

c) Ensure a more outcome-oriented and operational approach to policy implementation to further mitigate ML/TF risks by leveraging existing co-ordination to capture implementation results from action plans and ensure these are systematically fed back into future risks assessments, prioritisation and policy development, thereby strengthening a shared and coherent understanding of risk mitigation across authorities.

Overall Conclusions on IO.1

Türkiye has a generally good understanding of its ML/TF risks, supported by a comprehensive and data-driven NRA process and continuous analytical work co-ordinated by MASAK. The assessment process is based on a common and well-resourced methodology that combines quantitative and qualitative data and is sustained through the Threat and Vulnerability Working Groups, which include all relevant competent authorities and private-sector representatives. The country's risk understanding includes the findings of its three NRAs (2019, 2023 and 2025) and separate legal persons and arrangements and NPO risk assessments. At the same time, some aspects of the risk understanding could be strengthened, including the full articulation of cross-border ML/TF dynamics, real estate sector risks, the role of trade-based mechanisms, and the risks associated with foreign-created legal persons and arrangements.

In addition, while TF risk understanding is strong in relation to identified threat actors, it is more limited in capturing how TF risks materialise across financial and non-financial channels, particularly beyond designated organisations and sanctions-focused frameworks. The treatment of cross-border cash risks could also be further developed, particularly in ensuring that available data is consistently reflected in the broader risk picture, and risk understanding is uniformly reflected across all sectors, including DNFBPs.

Overall, Türkiye has achieved a high level of policy coherence and institutional co-ordination, including through its National AML/CFT Strategy, which requires all agencies to align with NRA findings. Co-ordination mechanisms are well established and support information sharing, joint analysis and the development of risk-informed policies and actions. This is reflected in the alignment of strategic priorities, legislative developments, supervisory approaches and operational activities with identified risks, as well as in strong inter-agency engagement. While co-ordination frameworks are robust and produce a wide range of outputs, there is scope to further strengthen the translation of these efforts into measurable outcomes and to ensure that system-level risks are consistently integrated into both strategic and operational responses.

Türkiye is rated as having a Substantial level of effectiveness for IO.1.

Immediate Outcome 1

1.1. Country's identification, assessment and understanding of its ML/TF risks

99. Türkiye has a generally good understanding of its ML/TF risks, supported by a comprehensive and data-driven NRA process and continuous analytical work co-ordinated by the FIU. The assessment process is based on a common and well-resourced methodology that combines quantitative and qualitative data and is sustained through the Threat and Vulnerability Working Groups, which include all relevant competent authorities and private-sector representatives. The country's risk understanding includes the findings of its three NRAs (2019, 2023 and 2025) and incorporates emerging threats identified through typology and strategic analysis reports.

100. The 2025 NRA has continued to evolve Türkiye's risk assessment methodology and introduced a 40 criteria quantitative scoring framework integrating 2021–2024 case data and linking results directly to an operational Action Plan for 2025–2026. This approach provides a dynamic, cross-sectoral picture of

national ML/TF risks, supported by regular inter agency co-operation and information exchange. Complementing the NRA, Türkiye's LPRA assesses vulnerabilities associated with the misuse of company structures, sectoral exposure and BO information. Similarly, Türkiye also conducted a separate assessment of NPOs as described in IO.10.

1.1.1. ML risks

101. Türkiye's understanding of cross-border ML/TF risks remains developing. The NRA treats TBML, sanctions evasion and smuggling largely as extensions of predicate offences, rather than standalone systemic risks. For example, given the size of Türkiye's informal economy (29–30% of GDP) and extensive cross-border trade flows, this approach may understate exposure to ML through trade finance, logistics chains, manufacturing exports, and commodity trading. Limited sectoral differentiation constrains understanding of how proceeds from organised crime and corruption integrate into legitimate activity. TBML risks per company types and economic sectors are nevertheless assessed in the LPRA which is a complementary exercise of the NRA. Further strengthening of risk understanding would benefit from more granular and systematic analysis of cross-border dynamics, particularly in relation to trade, smuggling, and associated financial flows. While Türkiye's role as a regional trade and transit hub is well recognised, deeper use of quantitative and qualitative data—covering trade finance, shipping activity, customs controls, logistics and cargo operations, and cross-border cash or value movements—would enhance the ability to fully assess and mitigate these risks. There is also scope to further strengthen the analysis of certain risk areas, including corruption-related risks, by more systematically incorporating findings from recognised international sources to enhance the analysis and deepen the overall understanding.

102. Türkiye's risk understanding also reflects awareness of the evolving and transnational nature of ML threats. Authorities recognise that foreign predicate offences, organised crime groups, and professional enablers exploit similar vulnerabilities, reinforcing the country's exposure to external risks. At the same time, there is growing recognition of the interlinkages between ML and TF risks, particularly in relation to cash-based activity, informal or cross-border financial flows, and organised criminality. Efforts to look beyond case-based evidence—by examining sectoral exposure, typologies, and emerging trends—indicate a more forward-looking approach to risk identification. This is illustrated by the identification of shifts toward virtual assets in drug trafficking, reflecting an understanding of how criminals adapt to technological developments and regulatory gaps, and highlighting areas where risk mitigation frameworks will need to continue evolving.

Table 1.1. Main ML risks identified by Türkiye, most abused sectors and methods

Offence	Predominant Sector	Other Sectors Abused	Primary ML Methods
Fraud	Banking, VASPs	PEMIs, REAs, jewellery, car dealerships, legal betting platforms, exchange offices	Domestic/international fund transfers, purchase of assets for conversion and/or disguise, front companies, cash transactions, front accounts, Point of Sale (POS) transactions
Illegal Betting and Gambling	Banking, PEMIs	VASPs, real estate, front companies, car dealerships	Cash transactions, Domestic/international fund transfers, purchase of assets[21] for conversion and/or disguise, front companies, cash transactions, front accounts, POS transactions
Drug Trafficking	Banking, VASPs	REAs, car dealerships, jewellery, EOs	Cash transactions, Domestic/international fund transfers, purchase of assets for conversion and/or disguise, front accounts, POS transactions
Theft and	Car dealership	Banking, REAse, jewellery,	Purchase of assets for conversion and/or disguise

[21] Purchase of assets includes all kinds of purchases made for conversion purposes (crypto assets, securities, real estate, etc.).

Offence	Predominant Sector	Other Sectors Abused	Primary ML Methods
Robbery		PEMIs, retail trade	
Smuggling	Abuse of Legal Persons, Banking	REAs, shipment, car dealership	Domestic/international fund transfers, purchase of assets/foreign currency for conversion and/or disguise
Forgery	Car dealership	REAs, Banking, front companies, notaries; VASPs	Purchase of assets for conversion and/or disguise, Domestic/international fund transfers
Corruption	Banking, Abuse of Legal Persons,	REAs, car dealership, PEMIs, associations	Domestic/international fund transfers, purchase of assets for conversion and/or disguise, Accounting
Tax Evasion	Banking	Abuse of legal persons, REAs, car dealership, EOs	Domestic/international fund transfers, Accounting, purchase of assets for conversion and/or disguise
Migrant Smuggling, Human Trafficking	Abuse of Legal Persons, Banking	Car dealership, banking, REAs, jewellery, EOs	Domestic/international fund transfers, purchase of assets for conversion and/or disguise
Usury	REAs (Banking,PEMIs– in case of POS Usury)	Car dealerships, front companies; insurance, rent-a-car	Cash transactions, purchase of assets for conversion and/or disguise, Accounting,

Source: Türkiye's NRA 2025, p. 90.

1.1.2. TF risks

103. Türkiye's TF risk understanding is strongly prioritised around threats posed by FETÖ, PKK/KCK–PYD/YPG, ISIL, AQ and their networks, as well as risks linked to FTFs and cross-border financial flows. While detailed and operationally informed, this actor centric focus may limit a cohesive picture of how TF enters and moves through the financial and non-financial system, especially for methodologies involving trade activity, informal value transfer systems and foreign linked channels.

104. Türkiye demonstrates a strong central understanding of TF risks, supported by MASAK's analytical capabilities and access to a wide range of financial and non-financial information. This understanding extends to a range of financing channels, including the use of cash, informal transfer mechanisms, virtual assets, and abuse of legal persons. The NRA identifies the abuse of NPOs for TF purposes as generally low risk, while recognising higher exposure for humanitarian organisations operating near conflict zones or vulnerable to impersonation, reflecting an understanding of specific sectoral vulnerabilities. However, overall understanding is more developed in relation to known threats and is less clearly demonstrated with respect to those involving non-designated actors. In addition, while linkages between TF, ML and other forms of criminal activity are recognised, there remains scope for improvement and how these interconnections may manifest in practice. TF risk understanding is not consistently reflected across supervisory authorities where the articulation of TF risks—particularly beyond sanctions-related obligations varies and is in some cases more limited. Authorities demonstrate practical understanding of TF risks inherent in Türkiye's geography—long standing smuggling corridors, overlapping licit/illicit trade flows and complex migration routes. These interlinked dynamics are not yet fully reflected in formal risk assessments and would benefit from further expansion and analysis to strengthen a more comprehensive and forward-looking understanding of TF risks and improve the identification of relevant indicators.

105. Strong interagency co-ordination and information-sharing mechanisms support Türkiye's understanding of TF risks. Authorities draw on a wide range of inputs—including financial intelligence, law enforcement information, intelligence sources, and cross-border data—and collaborate closely through established co-ordination structures, joint investigative approaches, and shared analytical platforms. This facilitates the identification of TF typologies and trends and contributes to a well-developed and operationally informed understanding of TF risks across relevant authorities. Efforts to raise awareness of TF risks, including through guidance and outreach, have contributed to an improved understanding of

certain TF vulnerabilities. However, this understanding remains uneven and is often more closely linked to compliance with targeted financial sanctions obligations.

106. TF risk understanding across the private sector varies across sectors and institutions. Banks generally demonstrate a more developed understanding, while other financial institutions, VASPs and DNFBPs show a more limited articulation of TF risks, often focused on targeted financial sanctions obligations. This is more evident among DNFBPs and smaller entities, where TF is less consistently identified as an inherent risk. As a result, the overall level of understanding is not uniform across sectors and is less developed in some higher-risk areas, which may affect the extent to which TF risks are identified and assessed in practice.

Table 1.2. Main TF risks identified by Türkiye, most abused sectors and methods

TF Risk Factor	Predominant sector	Other Abused Sectors	Predominant TF Methods
FETÖ	Banking	Front company abuse in the retail sector, PEMIs, VASP[22], NPOs.	Collecting, providing, using funds under the names of money transfer, donation, himmet etc., physical cash supply and courier activities, VAs abuse
PKK and Factions	Banking	Front company abuse in the retail sector, PEMIs, EOs, jewellers, NPOs, REAs, VASP and cultural activities.	Collecting, providing, using funds under the names of money transfer, extortion, tax etc., smuggling, cash supply and courier activities, hawala, supply of weapons, illegal sources of finance, abuse of VAs, sales of publications
Tos Abusing Religion	Banking	PEMIs,VASP, EOs, NPOs, jewellers, cash courier activity, front company abuse in the retail sector	Domestic and/or international fund transfer, transactions for raising, providing and using funds especially through the Internet, hawala transactions, abuse of VAs.
Leftist Terrorist Org.	Banking	Cash courier activity, Cultural publications	Transactions for raising, providing and using funds, cash transactions, courier activity, sale of cultural publications

Note 1: Türkiye includes in the category of "terrorist organisations that abuse religion" AQ and ISIL, and their factions which are mentioned in UNSCR 1267(1999),1989(2011) and 2253(2015). Also, risks associated with FTFs mentioned in different UNSCR including 2170(2014), 2178(2014), etc., in the FATF methodology criteria 5.2bis , and so-called lone wolf.
Note 2: This category covers DHKP/C, MLKP, TKP/ML, MKP, DKP/BÖG and the other Leftist Organisations which aim to destroy the current constitutional order by means of an armed civil Insurrection.
Source: Türkiye's NRA 2025, p. 90.

1.2.3 Cross-cutting ML/TF risks

107. Türkiye's ML/TF risk understanding is strong and evidence based; however, there are cross-cutting gaps in the overall risk picture that indicate that certain high-risk channels are not yet fully captured within the NRA framework. Insights drawn from across the assessment point to uneven incorporation of system-level risks. In particular, the assessment highlights that TF STR reporting remains disproportionately low across several high-risk sectors—especially MVTS, exchange offices and VASPs—despite their central role in Türkiye's ML/TF typologies. This suggests uneven risk recognition and under-reporting in sectors where cash-intensive activity, foreign-linked flows and unlicensed operations persist despite measures to detect these.

108. Gaps remain in fully capturing vulnerabilities related to complex ML schemes involving foreign predicate offences, the misuse of multilayered legal person structures, trade-based mechanisms, and the role of legal and accounting professionals. These patterns involve sophisticated layering, cross-border integration, and the use of shell or front companies that are not consistently reflected in the NRA or LPRA. In addition, there are gaps in the understanding of cross-border cash smuggling risks, where high declaration volumes are not matched by seizures or follow-up investigations, and limited dissemination of customs data constrains integration into the broader risk picture.

109. Cross-cutting limitations are also evident in the extent to which DNFBPs understand ML/TF risks. While national level risk understanding is generally good, this does not translate consistently across DNFPB sub-sectors. Risk awareness is uneven – more developed in some sectors than some others, and TF risk understanding is particularly weak across the DNFPB segment.

110. There are also ongoing gaps in the understanding of ML/TF risks associated with foreign-created legal persons due to an analytical aperture that constrains the scope of risk analysis, as well as insufficient cohesion between risk identification, assessment, and understanding. In parallel, gaps persist in the identification, assessment and understanding of risks related to foreign-created legal arrangements, as current processes do not fully capture how such structures may be used in practice, particularly in cross-border contexts, limiting a comprehensive and forward-looking view within the national risk framework.

111. Taken together, these cross-cutting gaps demonstrate that, while Türkiye's national risk understanding is generally robust, system level insights from financial intelligence (IO.6), ML investigations (IO.7) and asset recovery/cash controls (IO.8) are not yet fully integrated into the national assessment and understanding of risk, particularly concerning foreign linked ML schemes, unlicensed MVTS, professional facilitators and cross-border cash movement vulnerabilities.

1.2. National policies and activities to address identified ML/TF risks

1.2.1. Policies and activities to address ML/TF risks

112. Türkiye's AML/CFT policies broadly align with NRA identified risks. The AML/CFT Strategy (2021–2025) as the main guiding document is embedded in a Presidential Decree, demonstrating utmost level of priority. The National AML/CFT Strategy focuses on improving detection, prevention and confiscation outcomes. For example, by directing the setting up of national multidisciplinary joint investigation teams according to subject matter expertise, especially regarding fraud and illegal betting and gambling and requiring all law enforcement agencies to prepare or update financial investigation guidelines in line with the findings of the NRA.

113. Authorities conducted extensive outreach, typology dissemination and training across all sectors to further reinforce alignment with risks identified.

114. As part of its ICRG action plan, Türkiye developed a separate Strategy Document on CFT and an accompanying Presidential Circular (No. 2022/13) in July 2022. The CFT Strategy and the Circular, which are to be updated on an ongoing basis as needed, emphasise and prioritise CTFT as an essential part of combatting terrorism, including through investigations and prosecutions, and conducting a study of Türkiye's capacity to combat TF and on the abuse of VAs for TF purposes. Work stirred by these two strategies is complemented by longstanding actions to combat other predicate offences and contextual factors such as drug trafficking, migrant smuggling, organised crime and the informal economy, which refer to preventive efforts as well as proceeds of crime. For example, the National Strategy for Combatting Drugs includes training by MASAK to LEAs staff.

115. Other priority actions operationalise the NRA-identified high-risk predicates—especially illegal betting/gambling, abuse of VASPs, misuse of POS systems and organised crime. These risks are embedded in Türkiye's AML/CFT Strategy and the 2023/2025 NRAs action plans, and are implemented through whole-of-government co-ordination mechanisms (notably the CBCFC and the Strategy Document working groups). Concretely, Türkiye is developing dedicated action plans for illegal betting and fraud; expanding typologies and STR scenarios (including risky VAs/PF indicators); applying risk-based supervision to payment/e-money institutions, VASPs, and merchant-acquiring channels vulnerable to POS abuse; and strengthening PFIs and confiscation practices through LEAs and judicial guidelines and organised crime.

116. On fraud, Türkiye's top predicate offence, a Fraud Prevention Research Report and draft national action plan were prepared focusing on education and awareness, strengthening of legal infrastructure and actions undertaken (so far) included recommending certain enhanced measures (e.g. approval by senior manager and transactional limits) for VASPs onboarded by banks.

117. On illegal betting and gambling, identified as the second major predicate offence, Türkiye adopted a strategy document (Presidential Circular No. 2025/18) instructing detection and intervention in electronic communications and virtual environments, along with focus on awareness and international co-operation.

118. Türkiye also adopted important legislative amendments in line with risks identified regarding payment services providers, virtual assets, stablecoins and both physical and virtual points of sale. For example, in 2021, following identified risks and misuse of payment services, Türkiye limited the use of prepaid cards in some instances (e.g. by requiring physical presence of cardholders or a Trusted Certificate for e-commerce) reducing prepaid card use in illegal betting and gambling.

119. Despite alignment of the AML/CFT strategy with risks, there are areas that need further development, such as strategies towards the real estate market. The use of the real estate market, especially for ML, is high as noted in Türkiye's 2025 NRA. However, the real estate framework—although comprehensive on paper (e.g. real estate agents are covered by AML/CFT obligations)—does not fully reflect how the market operates, as many transactions occur directly between buyers and sellers without intermediaries. This limits the practical reach of AML/CFT obligations of real estate agents as reporting entities and needs further reflection.

120. AML/CFT obligations in Türkiye extend beyond FIs, VASPs and DNFBPs, to other non-financial entities such as car dealers, postal and transportation service (e.g. cargo companies), sports clubs, lotteries and bets, considering ML/TF risks identified by Türkiye. Car dealers (purchase-sale of motor vehicles and showroom) have been identified as an important method to launder proceeds of theft and robbery (Among the top 5 predicate offences; 5th in 2023, 4th in 2025). In addition, to mitigate abuse of the sector further, authorities established a "Secure Payment System" in February 2020 mandating payment of purchases through banking and payment institutions and with assistance of a Notary.

1.3. Exemptions, enhanced and simplified ML/TF measures

1.3.1. ML/TF measures

121. Türkiye does not have exemptions from compliance with the FATF Standards and applies AML/CFT obligations, as noted above, to other sectors in line with its ML/TF risks.

122. Türkiye applies enhanced and simplified due diligence (EDD, SDD in some cases, as provided for in the RoM (see R.1 and R.10) in line with its ML/TF risks and FATF R.10. SDD is not permitted where ML/TF risk might occur. Türkiye demonstrates good use of NRA results to calibrate EDD and SDD. Updated STR typologies and guidance further show risk responsive adjustments.

123. On EDD, examples include removing POS/virtual POS from SDD eligibility due to misuse and tightening EDD for VASPs (MASAK Communiqué No. 29 and RoM) including through introducing cooling off periods. Virtual assets purchased cannot be transferred within 48 hours of purchase and withdrawals cannot be made before 72 hours.

124. On SDD, following the 2023 earthquake that affected many of Türkiye's provinces, different means of identification were added to Communiqué No. 5 to facilitate CDD and access to financial services. In addition, after its 2025 NRA and in line with the FATF's changes to R.1(though Türkiye is not yet being assessed against this aspect of the Methodology), MASAK issued new SDD measures and updated the Frequently Asked Questions (FAQ) section in its website clarifying related AML/CFT obligations.

125. However, gaps remain in applying enhanced measures to trade related ML, cross-border cash flows and informal MVTS. Evidence that supervisory authorities integrate these risks consistently into prioritisation remains limited. Evidence that supervisory authorities integrate these risks consistently into prioritisation remains limited Some variation remains in how risk understanding is translated into supervisory and preventive outcomes, particularly in the consistent application of risk-based prioritisation across sectors and in ensuring that supervisory responses fully reflect the scale and nature of underlying risks.

1.4. Objectives and activities of competent authorities and SRBs

126. Since the 2019 MER, Türkiye has significantly strengthened alignment of competent authorities and self-regulatory bodies (SRBs) objectives and activities with national AML/CFT policies through the AML/CFT Strategy, which is a binding and cohesive document requesting support of all public institutions and organisations (including some SRBs with public function such as the Union of Notaries Public) to carry out their responsibilities within the Strategy and enhanced the FIU leadership. Ministries and regulators integrated NRA findings into operational policies, supervision manuals, and investigative guidance as shown throughout the following Chapters (see IO.3 in particular on implementation of risk-based supervision and IO.7 on dedicated resources including special courts for ML cases). All competent authorities and some SRBs have also participated in NRA exercises and Threat and Vulnerability working groups.

127. Threat and Vulnerability working groups allow for AML/CFT policies to be collaboratively developed by taking into account the ML/TF risks identified, including through the FIU's strategic analysis.

128. However, SRBs show uneven implementation of risk-based obligations, and operational alignment in areas such as informal economy risks remain weaker. To fully demonstrate effectiveness, SRBs should more systematically embed NRA findings into licensing, fit and proper assessments, thematic reviews, inspections, and sanctions.

1.5. National co-ordination and co-operation to develop and implement policy

129. Co-operation and co-ordination on AML/CFT policies in Türkiye are anchored in a Presidential mandate (the AML/CFT Strategy) requiring all agencies to align with NRA findings. MASAK chairs the Threat and Vulnerability Working Groups, which meet frequently and bring together over 30 competent authorities. The 2025 NRA sets out several multi agency action plans—covering illegal betting, fuel smuggling and abuse of NPOs for TF purpose—which demonstrate clear co-ordination and defined deliverables. There is generally robust co-operation among competent authorities, particularly between the FIU and LEAs, supported by ongoing communication and structured engagement through these

working groups. This co-operation is also reflected in regular interactions with public prosecutors across provinces.

130. There is some evidence of cross-cutting adoption of best practices, such as lessons from the 2018–2021 fuel smuggling initiative informing the 2023–2025 tobacco smuggling plan. However, Türkiye's co-ordination remains largely output focused. While mechanisms produce valuable activities—meetings, training sessions, typology reports, and action plans—there is limited evidence of how these efforts translate into measurable reductions in ML/TF risk. A more outcome-oriented approach would enable Türkiye to assess progress against defined objectives, strengthen learning and adaptation, and ensure that existing reforms are used to their fullest potential.

131. Greater use of the Department of Smuggling, Intelligence, Operation and Data Collection (KİHBİ[23]) platform (e.g. through structured and regular engagement) could further strengthen the operationalisation of policy implementation by systematically consolidating outcomes from action plans, aligning priorities across competent authorities, enabling cross-sectoral visibility of how risks are addressed, and ensuring that implementation results are translated into a shared understanding of risk mitigation in practice, and ensuring that these results are consistently translated into a shared and coherent understanding of ML/TF risks and progress. While outcome data is collected to some extent, its use to inform a common operational picture and strategic direction across authorities appears more limited in practice. In particular, greater use of the Department of Smuggling, Intelligence, Operation and Data Collection (KİHBİ) platform (e.g. quarterly meetings) could also facilitate system wide reflection on lessons learned, alignment of priorities, and more strategic future policy development. KİHBİ is the entity responsible for co-ordinating anti-smuggling activities, improving inter-agency co-ordination and ensuring the guidance of the relevant authorities and is also in charge of monitoring, co-ordinating and evaluating the National Strategy Document and Action Plans on the Fight against Organised Crimes.

1.6. National co-ordination and co-operation for operational purposes

132. Since the 2019 MER, Türkiye has enhanced its mechanisms for inter-agency co-operation and co-ordination for AML/CFT operational purposes. Türkiye maintains a structured and functioning co-ordination system, anchored in the AML/CFT Strategy and Action Plan, and reinforced through a network of dedicated working groups and inter-ministerial forums. The Threat Working Group—comprising the Ministries of Justice, Interior, Trade, Treasury and Finance, Environment and Urbanization, and law enforcement agencies (TNP, GGC, and Coast Guard)—serves as a standing operational co-ordination forum for emerging threats. The Case Working Group, established in 2021, follows up on complex ML/TF cases and supports FATF-related submissions, having convened 25 times since its inception. Moreover, high-level and practitioner-level co-ordination meetings, many led by Deputy Ministers from the Ministries of Treasury and Finance (MoTF), MoJ, MoI , MoT, and MoFA, have institutionalised co-operation on legislative alignment, case management, statistics, and operational improvements.

133. FIUs co-operation with LEAs has also become more operationally focused. FIU–LEA feedback mechanisms are now formalised through protocols and operationalised via the working groups. LEAs are required to report on follow-up actions stemming from FIU disseminations, and the FIU has increased the volume of joint trainings and typology-based workshops with public prosecutors and LEAs since 2023, promoting two-way information flow. The NRA is now fully integrated into operational decision-making, as evidenced by the Ministry of Justice Circular No. 155/1 (2021), updates to financial investigation and supervision guidelines, and the use of NRA results in prioritising investigations and prosecutions. These

[23] KİHBİ is the entity responsible for co-ordinating anti-smuggling activities, improving inter-agency co-ordination and ensuring the guidance of the relevant authorities and is also in charge of monitoring, co-ordinating and evaluating the National Strategy Document and Action Plans on the Fight against Organised Crimes.

developments collectively demonstrate an improvement in Türkiye's ability to co-ordinate and co-operate for operational purposes.

134. Co-ordination relies heavily on MASAK for financial analysis in complex cases, indicating more limited capacity within LEAs to independently conduct PFIs. In addition, co-ordination is uneven across authorities, with more limited operational contribution from agencies such as Customs Enforcement and the Coast Guard, particularly in higher-risk areas such as cross-border currency movements, smuggling and the informal economy, which affects the overall effectiveness of co-ordinated responses in these areas. Moreover, while co-ordination has matured around the highest-risk areas identified in the NRA (organised crime, fraud, and illegal betting), cross-cutting systemic risks—such as those linked to the informal economy—require stronger operational co-operation. The Action Plan for Combating the Informal Economy (2023–2025) provides a solid policy basis, but its operational implementation, especially among fiscal, trade, and enforcement authorities, remains less advanced compared to case-based co-operation.

135. Türkiye also demonstrates strong and well-institutionalised operational co-ordination for TF. Public prosecutors play a central co-ordinating role within Türkiye's operational framework, supported by specialised LEAs, MASAK and intelligence agencies, with the systematic application of parallel financial inquiries in terrorism cases. Co-ordination is further strengthened through extensive information-sharing mechanisms, integrated databases (e.g. UYAP), and the use of ad hoc joint investigation teams. Competent authorities make use of a wide range of domestic and international information sources, and operational co-operation is supported by specialised units, regular inter-agency engagement and strong data integration capabilities, enabling timely detection and co-ordinated investigative responses. Operational co-ordination is generally effective, particularly in cases involving domestically designated and UNSCR-listed terrorist organisations but could be strengthened for more complex TF typologies. In addition, co-ordination across all relevant authorities, including those with responsibilities in cross-border and trade-related contexts, could be further enhanced to support a more consistent operational response across the full range of TF risks. Overall, while co-ordination mechanisms are strong, further enhancements in these areas would support a more comprehensive and forward-looking operational approach.

2 International co-operation

The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this chapter are R.36-40 and elements of R.9, 15, 24, 25 and 32.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Türkiye has a sound legal basis to provide and seek the widest possible range of MLA, including extradition, in relation to ML, associated predicate offences and TF.

b) Türkiye provides MLA and extradition in a constructive way, with generally good quality of assistance and demonstrated capacity to support foreign investigations, provides good quality information/statements for prosecution and conviction and facilitates asset recovery, particularly in ML, terrorism and TF cases. Except where a country spontaneously provides feedback to Türkiye, there is no mechanism to evaluate and consequently improve upon the quality of MLA provided.

c) Delays which deviate from standard processing timelines in MLA execution are primarily due to intricate demands of cyber-investigations—such as IP address tracking—and the inherent complexity of multiple requests or requests involving numerous parties.

d) While a limited proportion of incoming extradition requests were granted by Türkiye, there is no evidence to suggest that requests were arbitrarily refused.

e) Türkiye actively seeks international co-operation and issues a high volume of outgoing MLA and extradition requests broadly in line with its risk profile. However, there is infrequent follow up by Türkiye regarding delayed responses from requested countries and inconsistent use of international co-operation to pursue assets abroad[24].

f) Türkiye demonstrates effective and appropriate use of other forms of international co-operation mechanisms to seek information for AML/CFT purposes (including BO information) in particular through MASAK, supervisory authorities, LEAs, customs authorities and tax authorities. Operational co-operation is well established and supports domestic action to initiate requests to or respond to foreign authorities. Police-to-police co-operation is a major strength in Türkiye's international co-operation framework, including through use of liaison officers, ad hoc meetings and sometimes police co-operation in parallel with MLA to avoid delays, as demonstrated through case studies (see especially Chapters 6 – 8).

[24] During the onsite visit, Türkiye advised of its strategy to enhance international co-operation through improvement of the Central Monitoring System (MİS), expansion of specialised judicial co-operation units, strengthening human resources and asset recovery training, providing data tracking and automation as well as increased use of informal co-ordination mechanisms.

g) Türkiye provides other forms of international co-operation constructively across MASAK, supervisory authorities, LEAs, customs authorities and tax authorities through, inter alia, spontaneous disclosures and participation in joint investigations.

Recommended Actions

Türkiye should:

a) Develop and disseminate guidance to requesting states on factors that may affect the timeliness and effectiveness of the execution of MLA, extradition and informal international co-operation requests, including common procedural, legal and documentation-related issues. This could be achieved through a comprehensive review of its processes and operational procedures.

b) Actively and consistently resort to international co-operation to target illicit proceeds that have been moved abroad. This could be achieved through the adoption of strategies, processes and guidance that ensure MLA - or other co-operation where appropriate - is considered a priority in cases with a cross-border nexus.

Overall Conclusions on IO.2

Türkiye demonstrates a generally effective framework for international co-operation, supported by a clear legal basis and institutional arrangements that enable competent authorities to provide and seek MLA, extradition and other forms of international co-operation extensively. Competent authorities engage constructively with foreign counterparts and have exchanged a wide range of information, including evidence, financial intelligence as well as supervisory and BO information. Türkiye actively seeks international co-operation across a broad range of predicate offences and uses both formal and informal channels, such as police-to-police co-operation, to pursue criminals and criminal property as evidenced, among other ways, by case studies (especially Chapters 6-8). The AT has attributed significant weight to these in considering how well Türkiye achieves this outcome. Türkiye has also demonstrated the capacity to support foreign investigations and judicial proceedings, for instance, through the execution of seizure and confiscation measures.

International co-operation is more effective in higher-risk and prioritised areas, notably ML, terrorism and TF, where specialised expertise, prioritisation mechanisms and urgency procedures contribute to more timely execution of requests. Moderate improvements are however needed to address lengthy processing timelines for ML-related incoming MLA, mixed outcomes for incoming and outgoing extradition, infrequent follow-up of outgoing requests and inconsistent use of international co-operation to pursue asset recovery abroad.

Türkiye is rated as having a Substantial level of effectiveness for IO.2.

Immediate Outcome 2

136. Türkiye's international co-operation framework and outcomes have been considered in light of the jurisdiction's position as a major regional trade, transit and financial hub, which brings exposure to complex and evolving cross-border ML/TF risks, its alignment with NRA and key ML/TF risks, its sound legal basis for providing the widest possible range of MLA (as already noted in its 2019 MER), as well as improvements since its 2019 ME. The 2025 NRA highlights, among other areas, fraud, illegal betting and gambling, drug trafficking, smuggling, corruption and the misuse of legal persons as significant drivers of ML activity. These risks often involve TBML, foreign predicate offences, cross-border cash movements and the use of payment systems as well as VAs. TF risks are similarly associated with cross-border financial flows, informal value transfer mechanisms and geographically connected networks.

2.1. Providing constructive, timely and quality mutual legal assistance and extradition

137. Türkiye has a sound legal basis to provide and seek the widest possible range of MLA including extradition in relation to ML, associated predicate offences and TF. Türkiye is party to several bilateral agreements, although, based on reciprocity, no agreements or memoranda of understanding (MoUs) are required to provide co-operation. Technical enhancements, such as seven specialised judicial co-operation bureaus (CADIB), the UYAP system (official and secure digital platform where all judicial proceedings and data entered by officials during judicial proceedings are recorded and can be prioritised) and roll-out of a Central Monitoring System (CMS) launched under the EU Project on Improving International Co-operation in Criminal Matters for enhancing the management and tracking of incoming and outgoing requests, improved efficiency and co-ordination to some extent since Türkiye's 2019 MER.

138. Türkiye has also put in place supplementary guidance tools such as the Circular on the Issues to be Considered by the Judicial Authorities for the Proceedings of International Criminal Rogatory, Circular on the International Service of Documents in Criminal Matters and Circular on Issues to be Considered by Judicial Authorities on Extradition.

139. Significantly, since Türkiye's 2019 MER, 49 foreign countries and one international organisation have deployed 138 police liaison officers in Türkiye, through whom a significant portion of operational exchanges is conducted. Türkiye also has approximately 102 counsellors stationed abroad, who similarly play an important role in seeking and providing information. Additionally, there are law enforcement officers from other countries who are posted to Türkiye; an arrangement which facilitates, inter alia, the exchange of information. Information exchange and joint operations are conducted through these liaison officers whereby "Police Co-operation Meetings" and visits have been organised to ensure the successful and effective completion of operations and to enhance success to fight against international and transnational criminal organisations. In addition, a conference is held and has been held once a year with the participation of police liaison officers, providing an opportunity to convey their requests regarding operational and law enforcement co-operation. Furthermore, Türkiye has assigned specific contact points to address or serve as a desk for incoming requests from specific countries to also help improve quality and timeliness of responses.

140. As in the 2019 MER, competent authorities are required to maintain the secrecy and confidentiality of investigations and inquiries, with information exchange being secured through established measures and in line with the jurisdiction's legislative framework which includes the International Judicial Cooperation in Criminal Matters Law and the Turkish Criminal Procedure law.

141. Feedback from the Global Network members reflects that international co-operation with Türkiye is generally viewed as active and functional, with many countries describing co-operation as constructive and noting timely or satisfactory responses to requests. While some jurisdictions raised concerns about delays or legal and procedural hurdles - particularly in more complex judicial co-operation matters - the overall feedback indicates that positive co-operation experiences were more commonly reported.

2.1.1. Providing evidence and locating criminals

142. Türkiye provides MLA and extradition in accordance with a clear and comprehensive legal framework, applicable bilateral and multilateral treaties and co-operation on the basis of reciprocity. There are no legal impediments that prevent Türkiye from providing assistance in relation to ML, TF, terrorism or associated predicate offences, including for the purpose of asset recovery. Under the Directorate General for Foreign Relations and EU Affairs, the MoJ, serves as the Central Authority, within which a Bureau of MLA in Criminal Matters and a Bureau of Extradition operate. As of November 2025, the staff levels for the Bureau of MLA in Criminal Matters comprised 10 judges/experts, 1 department director, three chiefs, two statisticians and 33 clerks. While there is no evidence to suggest that this composition is inadequate for the volume of incoming requests, the Central Authority intends to conduct a review of its staffing complement in line with Türkiye's efforts (e.g. increase in ML/TF investigations as expressed in IO.7 and IO.9).

143. During the reporting period, Türkiye's Central Authority received a substantial volume of incoming MLA requests across a broad range of offences. As detailed in **Table 2.1** below, there were over 700 incoming MLA requests between 2021–2024[25] for ML, terrorism, TF and other major economic offences (including serious predicate offences).

Table 2.1. Incoming MLA Requests from 2021-2024

Category	Incoming MLA Requests
Money Laundering	186
Terrorist Financing	6
Terrorism (non-TF)	96
Other major economic offences	437
Total	725

144. Of the 186 ML-related requests, 80 were fully executed, 9 partially executed, 18 rejected and 79 remained pending at the end of the period, with an average processing time of approximately 161 days, which is considered by the AT as relatively timely for more complex requests but less so for expectations regarding simpler requests. While the rejection rate is low (approximately 10% of incoming requests were denied) and refusals were grounded in clear legal or procedural reasons, there is a considerable number of pending requests (approximately 42.5% of incoming requests). Most pending requests were however under active execution rather than inactive and the volume, intricate technological nature of some of the incoming requests and countries submitting several supplementary requests, amongst other factors, place operational demands on the system, which contribute to longer than average execution times for some categories of requests, particularly ML.

145. Incoming MLA requests related to terrorism and TF are prioritised, with the average response time for execution being 7.5 months, which as noted above tends to be in the higher, longer end for more complex matters and expected for TF. Türkiye received a limited number of TF-specific MLA requests and a higher volume of terrorism-related requests. These requests benefit from dedicated prioritisation tools,

[25] Due to an update on the UYAP informatic system and UYAP-2/3 integration, electronic capture and consolidation of statistics for 2025 was not possible.

specialised prosecutors and courts as well as electronic coding that flags urgency, resulting in faster execution compared to ML cases. This demonstrates Türkiye's ability to deliver timely assistance where risks are clearly identified and prioritised and where operational arrangements enable rapid processing.

146. Türkiye does not have a mechanism to seek feedback on the assistance it rendered; however the country provided several examples and newspaper articles of the positive feedback conveyed by assisted jurisdictions. Additionally, general accounts from the Global Network reflected that Türkiye has engaged collaboratively in the information exchange process, quality responses were submitted and critical assistance was provided. Furthermore, some jurisdictions reported that Türkiye's responses were provided in a timely manner with urgent requests being prioritised. **Box 2.1** includes examples of Türkiye's effective execution of MLA requests notwithstanding operational constraints.

Box 2.1. Successful execution of mutual legal assistance despite operational constraints

Case Study 1.

In 2021, Country X submitted an MLA request to Türkiye seeking bank account details and transaction records related to fraud proceeds transferred to an account located in Türkiye. The request was processed and fulfilled, with all relevant information and documentation transmitted to the competent authorities in Country X, demonstrating Türkiye's commitment to providing constructive, timely and quality assistance in line with FATF Core Issue 2.1. Notably, Country X also provided assurances regarding the protection of bona fide third parties in relation to potential seizure measures, highlighting an important safeguard in cross-border asset recovery efforts. However, the seizure request itself could not be executed due to the absence of funds in the account at the time the request was received. This case also involved procedural delays, as the request required location-related information (such as a postal or IP-related address), but the address initially provided by Country X was inaccurate. Consequently, the request had to be disseminated to Chief Public Prosecutors' Offices across three separate jurisdictions within Türkiye, extending the response timeline. Despite these operational challenges, Türkiye proceeded to fully co-operate and provide comprehensive feedback, underscoring its adherence to international co-operation standards and good faith engagement in MLA processes.

Case Study 2.

The suspect was accused of hacking various companies' information and ML, therefore the provision of documents and information was sought. Information about cryptocurrency records was also among the requested assistance. The requests were followed by supplementary requests over a period of time and after execution, authorities of the requesting country sent an email to show their appreciation.

Case Study 3.

The suspect was accused of murder. However, bank records constituted an important component of the request and was vital for the resolution of the case. Additionally, requested vital information and documents could not be used unless confirmed and approved by Turkish authorities. In this case, information and documents were successfully provided and the testimony of a witness, who was unable to attend trials in the requesting country, was provided via videoconference. An email from the requesting country's authorities regarding their appreciation and importance of Türkiye's assistance was provided.

2.1.2. Extradition

147. Extradition requests received by Türkiye are assessed and processed through a structured central authority framework led by the MoJ, with judicial determination by competent courts and the availability of appeal. The Bureau of Extradition is staffed with nine judges, one director, one deputy general director, five heads of departments, one chief clerk, 22 clerks, two statisticians and 2 archivists. Requests are examined against defined admissibility criteria, including minimum penalty thresholds, dual criminality, nationality restrictions and human-rights safeguards. Simplified extradition procedures are available and used in practice where consent is given, contributing to shorter timelines in such cases. **Table 2.2** identifies the number of simplified extraditions.

Table 2.2. Number of simplified extraditions (Categorised by region)

Country	2021	2022	2023	2024	2025	Total
Western Europe		1			4	5
Non- EU	1	2				3
Central Asia			1		1	2
Eastern Europe			1		1	2
Southeast Europe				1	1	2
Middle East				1		1
Total	**1**	**3**	**2**	**2**	**7**	**15**

148. Aside from the above simplified extraditions, during the reporting period, Türkiye received 75 incoming extradition requests related to ML, TF and terrorism offences, almost half of which were from countries with different extradition laws. As reflected in **Table 2.3**, which spans 2021-2025, a limited number resulted in surrender, while a significant proportion remained pending or disposed without extradition. From the descriptions and details provided, the AT appreciated that the reasons for disposal were beyond Türkiye's control, such as the withdrawal of an extradition request because an arrest warrant was lifted in the requesting country or the withdrawal of an extradition request because the statute of limitations for the offence had expired in the requesting country. Regarding the four rejected requests, the main grounds for refusal were legal constraints, notably the prohibition on extraditing nationals and the absence of dual criminality, which are consistent with international grounds for refusal. There is no indication that such requests were refused arbitrarily or without transparency.

149. Competent authorities report that simplified extradition procedures can result in surrender within approximately 180 days, while other requests averaged 594 days (less than twenty months), which demonstrates operational capacity in eligible cases. Pending cases remain constrained by several factors, such as, representatives raising objections in court matters. Other challenges include the requirement to locate and identify foreign nationals who enter through unofficial channels and use Türkiye to transit to other countries, lack of fixed residences or use of forged identification. Additionally, at times, Red Notices do not contain essential identity and personal information such as distinguishing features. In some cases, use of different alphabets leads to individuals being registered under different names in the Turkish system, resulting in matching difficulties. In all those instances, the fugitive status of such individuals necessitates extensive field operations to locate and identify them, given Türkiye's wide geographic expanse. Importantly, some extradition requests related to cases where the principle of *ne bis in idem* clearly applied in Türkiye, as individuals sought for extradition on grounds of being a member of ISIL were already prosecuted and convicted in Türkiye for being a member of ISIL, with their sentences being executed in Türkiye. These convicts, after the execution of the penalties, can be later subject to deportation measures. Furthermore, where part of the alleged offence has been committed within the jurisdiction, investigations are initiated in Türkiye against the persons sought for extradition.

Table 2.3. Incoming extradition requests

Category	Requests Received	Accepted/ Surrendered	Rejected	Pending	Withdrawn
ML	28	3	1	18	6
Terrorism	42	-	2	30	10
TF	5	0	1	4	0
Total	**75**	**3**	**4**	**52**	**16**

2.1.3. Facilitate asset recovery

150. Türkiye has demonstrated the capacity to enforce foreign seizure and confiscation orders and to maintain follow-up arrangements for ongoing restraint measures. Türkiye also has measures in place for the deduction or sharing of substantial or extraordinary costs associated with executing freezing, seizure, or confiscation orders. In this regard, legislation provides that unless otherwise agreed by the parties, costs incurred in executing a request for judicial co-operation are to be borne by the executing state (IJCL, art. 34).

151. During the reporting period, Türkiye received 82 requests relating to seizure and one for confiscation measures, of which 13 were finalised (executed or otherwise completed). In other cases, seizure or confiscation was not possible due to insufficient funds in the account, lack of causal connection, or absence of supporting documentation. Furthermore, where possible unlawful seizures arose, authorities followed provisions requiring a guarantee on allocation or reimbursement of possible damages (Criminal Procedure Law Article 141 and Law nr 6706 on International Judicial Co-operation in Criminal Matters article 3/3). In this regard, additional information and documentation were required from countries requesting the seizure in order to continue the proceedings. While some foreign countries acquiesced to this requirement, there were a few jurisdictions which did not. The case study in **Box 2.2** is an example of Türkiye's successful recovery of assets through co-operation at the behest of an international partner.

Box 2.2. Facilitating a request for confiscation

Case Study: Double (dual)

Türkiye received a request from Country X to locate and seize the assets of Individual A, who was investigated for drug trafficking and ML. After Türkiye seized the assets, Country X's court finalised its confiscation order, which Türkiye recognised and following co-operation and co-ordination to avoid double/dual enforcement, a final amount of EUR 736 650,86 was confiscated in 2024.

152. Türkiye has treaty-based mechanisms which facilitate the sharing of confiscated assets with other countries. Türkiye has entered into bilateral agreements with a number of countries—including China, Kazakhstan, Russian Federation, the United States and several others—which expressly allow for the sharing of confiscated proceeds resulting from judicial co-operation. In the absence of a treaty, Türkiye may still accept and act on co-operation requests on the basis of reciprocity (the analysis in c. 38.7 refers). Qualitative or quantitative information regarding the sharing of confiscated assets was unavailable, however **Box 2.3** provides examples of successful repatriation of assets.

Box 2.3. Confiscating and returning assets

Case Study 1

On 17 February 2025, the FIU of Country X requested the suspension of a financial transaction suspected to be linked to kidnapping and aggravated fraud, after a victim, Ms. J., had been manipulated into transferring funds to Türkiye. The scheme began on 10 February 2025, when a man falsely claiming to represent a national criminal investigation authority contacted Ms. J. and persuaded her that she could assist in apprehending organised fraudsters in Türkiye by purchasing an apartment allegedly used by the criminals. The following day, a woman purporting to be from INTERPOL reinforced the deception and convinced Ms. J. that she needed to travel to Türkiye to complete the transaction. Ms. J. travelled alone to a city in Türkiye, met the suspect at a hotel and remained there until 18 February 2025, during which EUR 291 000 was transferred to an account held by a Turkish national under the suspects' direction.

Following the FIU request, MASAK imposed a seven-working-day suspension measure on 19 February 2025 to prevent dissipation of the funds. A Financial Detection Report, prepared on 24 February 2025 and submitted to the Chief Public Prosecutor, concluded that no reasonable connection could be established between the suspect's financial profile and the transferred amount and assessed that the funds were likely proceeds of fraud. In the meantime, in March, a formal MLA request was received from Country X where the victim resides and same was evaluated and examined, in accordance with relevant legislation, by the Central Authority. In order to prevent dissipation, immediate contact was made with the FIU, as the request letter indicated suspension on the account. Subsequently, contact was made with the judicial authority which is authorised for seizure. On 14 March 2025, X City's Court of Peace ordered the seizure of the full EUR 291 000. When the request was transmitted to the relevant judicial authority, it was discovered that the proceeds of crime had already been returned to the victim. The authorities in X country were afterwards asked if they want to proceed with their request and a letter of acceptance of conclusion and appreciation was delivered as a reply.

Case Study 2:

In 2021, a request was received from an EU member country —one of the countries with which Türkiye collaborates most closely in the field of legal co-operation—to carry out a search and seizure at the Turkish address of a Turkish citizen under investigation for fraud. The request was immediately forwarded to the relevant Turkish judicial authorities for the purpose of obtaining information and documents. Meanwhile, a guarantee against unlawful seizure was requested from the EU member country authorities, and once this guarantee was received, the seizure request was immediately forwarded to the relevant judicial authority. Information regarding the seized items was promptly communicated to the EU member country and the items were handed over to officials at the EU member country Embassy for examination.

153. Türkiye maintains a clear legal framework and adequate operational capacity to deliver constructive and comprehensive MLA and extradition, including in support of foreign investigations and asset recovery. Authorities execute a broad spectrum of measures—such as collecting and transmitting evidence, financial and asset information (movable and immovable), criminal records, testimony (including via videoconference), transfer of proceedings and the implementation of seizure and confiscation orders, while engaging proactively with requesting jurisdictions to clarify issues and minimise refusals or partial execution. The system demonstrates particular effectiveness in terrorism and TF cases, where prioritisation mechanisms, specialised expertise and urgency coding facilitate expedited handling. Although processing times for ML-related MLA requests can at times affect timeliness and the proportion of incoming

extradition requests resulting in surrender is relatively limited, these outcomes are generally attributable to legitimate judicial, procedural and constitutional safeguards (such as the *ne bis in idem* principle explained above) rather than deficiencies in co-operation. Competent authorities obtain informal feedback on assistance rendered and address issues on a case-by-case basis, however the jurisdiction would benefit from performance monitoring so that any quality and timeliness issues could be proactively and appropriately addressed. Notwithstanding these moderate areas for improvement, the framework operates effectively in practice and demonstrates the provision of meaningful international co-operation.

2.2. Seeking appropriate and timely mutual legal assistance and extradition

2.2.1. Seeking evidence and locating criminals

154. Türkiye actively seeks international co-operation and issued a high volume of outgoing MLA and extradition requests over the period 2021-2024, reflecting a strong willingness to engage foreign counterparts. Türkiye provided the AT with extensive quantitative and qualitative data which demonstrated significant and varied use of outgoing MLA, both in stand-alone ML and TF cases and more extensively, in predicate offences and terrorism-related matters. Regarding stand-alone ML cases, Türkiye sent 38 requests to 18 jurisdictions. Of these requests, which touched and concerned underlying offences such as drug trafficking, fraud, illegal betting and gambling, human trafficking, establishing a criminal organisation/membership of a criminal organisation and tax evasion, nine were accepted, eight were rejected, one was partially accepted and 20 were pending. 6 649 MLA requests were generated pertaining to major predicates identified in the country's risk assessment. These requests covered offences such as fraud, forgery, theft and robbery, customs smuggling, usury, illegal betting and gambling and migrant smuggling. Of those, 2 794 were accepted and 2 763 are pending, with the remainder accounting for rejected or partially rejected outcomes. For terrorism and TF related cases, 1 131 and seven requests were sent, respectively. Of the seven TF requests, two were accepted, three rejected and 2 were pending at the end of the on-site. For the terrorism-related matters, there were 577 pending requests, 243 accepted requests, 302 rejected requests and 9 partially rejected requests. The statistics therefore reveal that while outgoing MLA is extensive and consistent with the country's risk profile, pending and rejected requests form a substantial share of outcomes.

155. Procedurally, if the relevant judicial authority detects an international connection in the case file, it will decide to submit an MLA request. For information such as criminal records, population registry data and bank account numbers that can be obtained through informal channels, judicial authorities are directed to informal channels by CADIB offices or the Central Authority. If the Central Authority reviews and approves that procedural requirements for a MLA request have been fulfilled, it forwards the file to the relevant country. In the interim, the Central Authority may remind the relevant judicial authority of other MLA instruments provided for in multilateral treaties and laws such as video conference. Alternatively, if a case involves a request against assets, it will be assigned a seizure code and cases assigned this code are reviewed and examined with urgency. These cases generally involve ML, TF and some predicate offences. Through the UYAP system, any requested file can be specially marked, casing a coloured alert to appear at the top of the screens of the experts responsible for the file's workflow. Files to be sent to MoJ through CADIB are also prioritised in this manner at the courts. Urgent requests are at times sought through police co-operation at the very beginning of the investigation (at times simultaneously with the MLA request) which prevents both delays and the loss of data. **Box 2.4** highlights an example of Türkiye's use of international co-operation channels to further active investigations.

Box 2.4. Case examples: Foreign predicate ML

Case Study

A complex transnational investigation dismantled multiple organised crime networks engaged in large-scale drug trafficking and the laundering of illicit proceeds. The case originated from financial intelligence analysis that identified sophisticated laundering patterns linked to narcotics distribution across several regions. From the outset, the investigation was built on extensive international judicial co-operation and co-ordinated law-enforcement action. Evidence derived from encrypted communication platforms—lawfully obtained and shared through judicial channels—proved central, enabling authorities to determine leadership and operational tiers, identify financial facilitators and trace cross-border cash. The operation was conducted in close partnership with Europol, Eurojust and INTERPOL, alongside numerous national authorities. Approximately 10 MLA requests and over 150 intelligence exchanges supported the investigation, complemented by operational co-ordination meetings to align prosecutorial strategies and evidentiary standards. Financial and asset-tracing intelligence further enabled investigators to connect drug trafficking proceeds to assets held across multiple jurisdictions.

Analysis of approximately 6 million encrypted messages identified more than 500 key accounts linked to organised crime actors, revealing a network of several thousand associated identifiers and illustrating the scale of the illicit operational network. Illicit proceeds were primarily moved through cash, precious metals and high-value goods, using laundering methods such as front companies, structured deposits, cash couriers and investments in real estate and commercial enterprises. A co-ordinated enforcement phase, involving several thousand officers across multiple jurisdictions, resulted in around 250 arrests, over 200 pre-trial detentions and the location of more than 10 internationally wanted individuals through INTERPOL channels. Asset recovery was a core objective, with authorities freezing or seizing properties, vehicles, corporate shares and financial accounts valued at over USD 355 million in Türkiye and various other countries. As the investigation expanded to over 300 suspects in Türkiye and various other countries, key lessons emerged: the critical role of MLA frameworks and joint investigation teams in ensuring cross-border admissibility of digital evidence; the importance of real-time operational co-ordination; and the effectiveness of parallel financial and narcotics investigations. The case underscores how integrating encrypted communication exploitation with financial intelligence can dismantle entire criminal networks while simultaneously targeting both operational capacity and illicit assets.

156. Türkiye has invested in improving, inter alia, the quality of outgoing requests through the establishment of CADIBs, detailed guidance and templates, a central monitoring system and extensive training of judges, prosecutors and clerks. These measures have strengthened the formal quality and legal completeness of outgoing co-operation requests and support constructive engagement with foreign counterparts.

157. Türkiye has underscored that average response times from foreign counterparts are long, particularly for seizure and confiscation-related requests. When there is a protracted delay, Türkiye undertakes follow-up on delayed outgoing MLA requests, including through periodic (annual) review of pending cases. However, such follow-up is not conducted through a structured, risk-based escalation framework with graduated timelines or scheduled interim tracking. As a result, although foreign response times are outside Türkiye's control, the limited frequency and formality of follow-up can impact time-sensitive and asset recovery cases where asset dissipation risks may be elevated.

2.2.2. Extradition

Year	Money Laundering					Terror Offence					TF				Total outgoing extradition requests/ year
	Accept	Reject	Pending	Disposed	Total	Accept	Reject	Pending	Disposed	Total	Reject	Pending	Disposed	Total	
2021	1	1	1	2	5		91	101	43	235	6	5	7	18	258
2022			1		1	1	69	67	38	175	1	2	3	6	182
2023			1		1	1	121	167	22	311	4	1		5	317
2024		2	6		8	1	157	570	18	746	2	8		10	764
2025			2		2		9	230		239		2		2	243
Total	**1**	**3**	**11**	**2**	**17**	**3**	**447**	**1135**	**121**	**1706**	**13**	**18**	**10**	**41**	**1764**

158. Türkiye actively seeks extradition and issued a very large number of outgoing extradition requests, particularly in terrorism-related cases as reflected in **Table 2.4**.

Table 2.4. Outgoing Extradition Requests: 2021-2025

159. The timely execution or low execution rate of outgoing extradition requests, particularly in terrorism related matters, should be viewed against factors outside Türkiye's control, including differing legal frameworks, asylum/refugee policies, judicial requirements and evidentiary thresholds applied in requested jurisdictions. As a result, while Türkiye demonstrates strong intent to pursue extradition, the practical impact of outgoing extradition remains challenging.

160. If the person is detained in the requested State for extradition purposes, the process is monitored continuously and periodically within the timeframes prescribed by the relevant extradition treaties. If the person sought for extradition is not detained in the requested State, inquiries are made through diplomatic channels and via Interpol, at intervals not exceeding three months, to ascertain whether the person is still in that country and to obtain updated information on the extradition proceedings. Proactively, in cases where Türkiye's extradition request is rejected, available judicial remedies are pursued, including appeals and review mechanisms, in order to challenge the rejection and seek reconsideration of the extradition. Accordingly, if there is no extradition request for the purpose of execution and if the extradition request is denied, the judicial authorities are instructed to seek judicial co-operation to finalise the case so that files currently in the investigation or prosecution stage can proceed to the execution stage. If requests that have reached the execution stage are denied, relevant authorities may be directed to file a request for transfer of execution, if the statute of limitations is approaching. In cases where neither of these conditions applies, the judicial authorities will continue to search for the individual until the statute of limitations expires. Furthermore, the use of alternative measures if an extradition request is denied typically occurs when the individual could be deported due to the lack of a valid residence permit.

2.2.3. Seeking to facilitate asset recovery

161. Türkiye has evidenced a clear legal framework and institutional capacity to pursue asset recovery through international co-operation and while the number of outgoing MLA requests specifically targeting assets abroad during the evaluation period (8 for seizure and 2 for confiscation) remains modest, the existing cases reflect a deliberate and targeted use of available mechanisms by competent authorities. Confiscation is established as a policy objective and as it pertains to asset tracing, depending on the case, outgoing information requests transmitted through the Egmont Group encompass a broad spectrum of financial intelligence inquiries—including STR and Suspicious Activity Reports (SAR) data, LEAs records, bank account information, transaction flows, BO and sectoral risk profiling. While "asset tracing" is not formally captured as a specific field within the EMIS system and therefore not statistically disaggregated,

internal estimates indicate that approximately 70% of such requests substantively relate to asset tracing objectives. Competent authorities have demonstrated the ability to generate tangible results in cross-border cases, as illustrated in **Boxes 2.4 and 2.5** and further examples in Chapters 7 and 8. Although the use of early freezing or restraint measures in outgoing requests has not yet been standardised, the functioning legal basis and demonstrated operational outcomes provide a solid foundation to enhance asset recovery efforts and further strengthen the effectiveness of international co-operation measures in this area.

Box 2.5. Recovering Assets

Case Study 1: Operation Exchange

A major drug trafficking and ML case was initiated by the Chief Public Prosecutor's Office of Province A following the detection of drug proceeds generated abroad and transported into Türkiye through couriers, then laundered via safe deposit boxes, real estate purchases and misuse of legal entities. The investigation, conducted by the TNP Narcotics Department in close collaboration with MASAK, became the largest of its kind in Türkiye's history. A comprehensive financial intelligence effort followed, with MASAK producing 17 analytical reports between 2019 and 2021, while LEAs applied surveillance, communication interception and undercover operations to refine the suspect network, leading to indictments against 73 individuals, including the organisation's leadership.

International co-operation was a central component of the investigation. To trace the suspects' overseas activities, Türkiye issued MLA requests to 8 countries, sought information from 23 countries through INTERPOL and exchanged financial intelligence with 21 countries via the Egmont Secure Web. These co-ordinated international efforts enabled the authorities to identify and restrain assets valued at approximately EUR 15 million, USD 15.8 million, GBP 6 million, TRY 121 million, as well as 160 real estate properties and 22 vehicles worth an estimated EUR 100 million. Substantial seizures were executed across financial and physical assets and the prosecution remains ongoing, demonstrating the effectiveness of sustained international co-operation in dismantling complex transnational laundering operations.

Case Study 2

MASAK submitted a request to Country Y regarding Individual X, who carried out acts of bid-rigging, qualified fraud and bribery, and have transferred high amounts of money to accounts in Country Y. In this context, a significant amount of information regarding person X was requested, and it was specified that bank account details, transfer transactions, current balances of the accounts and information on the further movements of the transfers received from Türkiye are required. In response to the request, Country X provided account statements and transaction information.

2.3. Seeking other forms international co-operation for AML/CFT purposes, including asset recovery

162. Beyond formal MLA, Türkiye generally makes extensive and appropriate use of other forms of international co-operation to seek information and assistance for inter alia, AML/CFT purposes, the identification of suspects, understanding complex ownership structures and supporting asset tracing. A broad range of competent authorities are involved, including FIU, LEAs, supervisory authorities and customs as well as tax authorities, each using channels relevant to its mandates.

2.3.1. FIU

163. MASAK plays a central role in seeking international co-operation through FIU-to-FIU channels, primarily via the Egmont Secure Web and where relevant, alternative secure arrangements with non-Egmont counterparts. MASAK demonstrated that it consistently seeks and receives a wide range of information, including financial intelligence, transaction data, account information as well as basic and BO information. Requests are clearly linked to a broad range of predicate offences, including fraud, drug trafficking, tax crimes, corruption, customs smuggling, illegal betting and gambling, TF, sanctions violations and virtual assets related offences; crimes which align with the risks identified under the NRA. In this context, requests are made to the relevant countries based on prioritisation in accordance with the Egmont Principles and FATF standards. MASAK's extensive direct access to domestic databases enhances its ability to formulate targeted requests and make effective use of information received from abroad.

164. MASAK's international co-operation is operationally embedded in its legislative framework and approximately 67 MOUs with foreign FIUs, (Egmont Group Members and non-members). Exchanges include incoming, outgoing and spontaneous submissions. This form of co-operation supports domestic analysis and operational decision-making and is not limited to reactive or ad hoc use**.** In the analysis, assessment and investigation of ML and TF offences, when foreign connections are identified regarding individuals and/or transactions, requests for information are made to foreign financial intelligence units promptly. When MASAK requests information from foreign counterpart financial intelligence units or shares information on its own initiative, there are rules that must be observed in accordance with national legislation and the Egmont Principles of Information Sharing. Furthermore, prioritising areas identified as high-risk through analyses and assessments conducted by MASAK or other competent authorities during information sharing enhances national effectiveness in combating ML and TF. In this regard, the following elements must be specifically considered and prioritised in both information requests and spontaneous sharing:

- Cases involving threat actors identified in NRA reports as having a medium or higher risk level regarding TF and ML;
- Cases involving sectors identified in NRA reports as having a medium or higher vulnerability risk level regarding TF and ML;
- Requests requiring the postponement of transactions;
- Requests involving legal entities identified as high-risk based on analyses and assessments conducted by MASAK or other competent authorities; and
- Requests for information that must be obtained urgently within the scope of the case under review, regardless of whether they fall under the categories listed above.

165. The responses to requests received provide relevant information that leads to the identification of the suspects involved in the case, the identification of the crimes and their value, the transmission of such information to prosecutors' offices, or the further expansion of the case based on the information received. This facilitates international co-operation by enabling the involvement of competent authorities in other countries, such as LEAs and prosecutors' offices. All incoming information is recorded in the system. If distribution authorisation is granted, all incoming spontaneous requests are forwarded to the relevant unit within MASAK for further review. Additionally, if there is a file in MASAK its owner is notified regarding all incoming information requests, regardless of whether they are still open or closed. Similarly, if the information request concerns a suspicious transaction report regarding a natural or legal person, multiple countries have made requests regarding the same natural person, or there are serious issues involved, this is also forwarded to the relevant analysis department. In addition, responses to requests for information are forwarded to the relevant department or unit that submitted the request, and, following the completion of the analysis, are also forwarded to law enforcement and judicial authorities, subject to distribution authorisation.

166. **Tables 2.5** and **2.6** detail outgoing requests by MASAK to Egmont and non-Egmont Group members, respectively, while **Table 2.7** provides an overview of the requests made for BO information. The case study at Box 7.2 in Chapter 7 (ML Investigations - Operation Comanchero) provides a practical example of the jurisdiction's collaboration with foreign partners.

Table 2.5. Number of outgoing information requests through Egmont Secure Web

Year	Outgoing Requests	Spontaneous Disclosures	Total
2021	368	1	369
2022	75	3	78
2023	99	2	101
2024	75	1	76
2025	164	0	164

Table 2.6. Number of Outgoing Financial Intelligence Exchanges with Non-Egmont Group Members

Requested country	2021	2022	2023	2024	2025	Total
East Asia	2	2	3	3	3	13
South Asia	2	0	0	0	1	3
Non EU	1	3	3	4	4	15

Table 2.7. Outgoing requests for BO information

Year	2021			2022				2023			2024		2025			Total		
Country	Request	Natural Person	Legal Person	Request	Natural Person	Legal Person	Request	Natural Person	Legal Person	Request	Natural Person	Legal Person	Request	Natural Person	Legal Person	Request	Natural Person	Legal Person
Non-EU				1	3	0										1	3	0
North America	1	0	2	1	4	0							3	0	4	5	4	6
North Africa	2	0	3													2	0	3
Northern Europe	4	0	11				2	9	2							6	9	13
Eastern Europe	16	2	330	1	4	0	2	11	14							19	17	344
South Asia	6	0	14										1	2	1	7	2	15
Western Europe	8	0	15				1	1	0				3	0	8	12	1	23
Central Europe	13	10	77													13	10	77
Southeast Asia	9	0	25										1	0	2	10	0	27
Middle East	3	1	8	1	1	1							6	1	30	10	3	39

Year	2021			2022				2023			2024		2025			Total		
Central Asia										1	0	2				1	0	2
Southern Europe	7	0	20													7	0	20
East Asia													2	0	4	2	0	4
East Africa													1	0	2	1	0	2
Total	**69**	**13**	**505**	**4**	**12**	**1**	**5**	**21**	**16**	**1**	**0**	**2**	**17**	**3**	**51**	**96**	**49**	**575**

2.3.2. Law enforcement agencies (LEAs)

167. LEAs seek information through police-to-police co-operation channels, including INTERPOL (as an example, 46 requests were sent in 2025), Camden Asset Recovery Inter-agency Network (CARIN) and liaison officers abroad, to obtain criminal intelligence, locate suspects and identify assets. See **Boxes 2.4** and **2.6** as well as Chapters 6, 7 and 8 (IOs 6-8).

Box 2.6. Case Study: Turkish National Police – Tracing the proceeds of drug trafficking

In connection with the laundering in Türkiye of proceeds derived from drug trafficking, which is a predicate offence committed abroad, a simultaneous operation was conducted in 2024 under the co-ordination of TNP Narcotics Department, targeting an armed criminal organisation led by X. The operation involved 79 locations across six provinces, with Y City as the central hub.

On the day of the operation, following the discovery of documents linked to EU-member country during a search of a suspect's residence, real-time intelligence was exchanged with EU member authorities. Furthermore, the answers provided by suspect Y to the questions posed were shared in real time with EU member country authorities as part of police co-operation. In this context, authorities in EU member country conducted searches of suspect Y's residence, workplace and rental safe deposit box in an EU member country and seized the 121.000 Euros in his bank account.

Furthermore, the digital data imaged during searches conducted by the EU member country judicial authorities was shared with the Narcotics Unit. As a result of the examination of the digital data, a connection was established between the seven vehicles and two properties located in Türkiye and the criminal organisation, and a money laundering report was sent to the Chief Public Prosecutor's Office in Y City.

As a result, the Y City Criminal Court of Peace seized seven vehicles and two properties, valued at 11.258.000 USD, that were under the suspect Y's control.

2.3.3. Supervisors of FIs, VASPs and DNFBPs

168. Supervisory authorities in Türkiye engage in international co-operation, to a moderate extent, to support both market supervision and AML/CFT objectives. For the BRSA, information requests are generally related to fit and proper processes for opening overseas branches and appointing senior executives. The Capital Markets Board (CMB), in particular, makes extensive use of the International Organization of Securities Commissions (IOSCO) Multilateral MoU, having concluded 54 co-operation agreements and exchanged information with numerous foreign supervisors on cases involving market abuse, unauthorised

capital market activities, fraud, VAs investigations and fit-and-proper assessments. The information exchanged—including ownership and partnership structures, personal and corporate data, account information and other supervisory-relevant intelligence with BO elements—demonstrates that international supervisory co-operation is effectively leveraged for AML/CFT-relevant purposes. CMB co-operates with foreign counterparts for various areas within its mandate, including the ongoing supervision of FIs, such as assessing fit and properness of supervised entities, which also contributes to AML/CFT objectives. In addition, the second paragraph of Article 257 of the Turkish Criminal Code (TCC) states: (2) Except in cases specifically defined as crimes under the law, a public official who, by neglecting or delaying the performance of their duties, causes harm to individuals or the public, or provides an unjust advantage to individuals, shall be punished by imprisonment for a term of three months to one year.

169. The CBRT requests the necessary information from the relevant authorities in the licensing processes of payment and electronic money institutions, as well as in cases where such information is required after licensing. If there are non-Turkish citizens or non-resident firms among the shareholders of these institutions, the CBRT requests intelligence regarding these individuals and companies from the relevant authorities abroad. Multinational companies operate in Türkiye's insurance and pension market and regular meetings are held with regulatory and supervisory authorities in the countries where the headquarters of these multinational entities are located. These meetings, referred to as "College meetings" are organised by the relevant authorities and facilitate information sharing among authorities within the framework of macro prudential supervision and oversight. For example, Y Insurance has its headquarters in Country B. Regular meetings are held under the supervision of the Central Bank of Country B. Another example is D Insurance Inc., a company headquartered in Country F that operates in Türkiye. Similarly, meetings are held with the relevant supervisory authority under the Central Bank of Country F. Furthermore, the exchange of information is not limited to the information and documents requested during the establishment phase; it also includes correspondence with the authorities of the relevant countries regarding the evaluation of submitted documents and the monitoring of the process, particularly in connection with share transfers.

170. Supervisory authorities (notably the CMB and the Insurance and IPRSA) also make targeted use of MASAK as an international co-operation channel, particularly in urgent cases involving foreign legal persons and share transfers requiring immediate supervisory action. This practice reflects effective domestic co-ordination and a risk-based selection of co-operation channels to ensure timely supervisory intervention (see **Tables 2.8, 2.9 and 2.10** as well as case studies in **Box 2.7**). MASAK has requested information regarding obliged parties from 14 foreign competent authorities in 2025 to enhance co-operation for supervisory purposes and this information is taken into account in the preparation of its 2026 supervision program. For the CMB, responses to information requests received from foreign countries are provided to the person assigned to the audited entity for consideration during the audit, and these matters are taken into account during the audit. In addition, information obtained regarding the obliged entity in the context of AML/CFT is reported to MASAK in accordance with the protocol signed with MASAK. For the BRSA, information exchange regarding fit and proper checks is directly linked to AML/CFT objectives because they ensure that individuals in key positions within financial institutions are trustworthy, competent and free from any criminal associations. It contributes to the risk mitigation efforts.

Table 2.8. Number of Information Requests Sent (CMB)

Country	Years					State of Request	
	2021	2022	2023	2024	2025	Yes	No
Central Europe					1	1	
North America	1						1
Western Europe			1				1
Southeast Asia			1			1	

Middle East	1					1	
Southeast Asia			1			1	
Middle East			1			1	
Northern Europe	1	1					2
South America			1			1	
Total	3	1	5		1	6	4

Table 2.9. Number of information requests sent (BRSA)

Country	Years					State of Request	
	2021	2022	2023	2024	2025	Yes	No
Middle East			3		2	5	
Southern Europe	1					1	
Northern Europe	1		1			2	
Total	2		4		2	8	

Table 2.10. Number of information requests sent (IPRSA)

Country	Years				
	2021	2022	2023	2024	2025
Middle East				1	
Southern Europe		1		1	
Central Europe			2		
Non EU	1			1	
Southeast Asia					1
Total	1	1	2	3	1

Box 2.7. Seeking of information by financial supervisors

Case Study 1

There was a request to transfer the shares of an insurance company established in Türkiye to a legal entity based in country X. In this context, a request for information was made by IPRSA to MASAK to promptly determine whether there was information regarding the beneficial owner and whether any investigations or similar proceedings have been conducted regarding these persons.

Note: In the event of a request from a foreign legal entity, the Institution contacts the authorities of the relevant country directly. However, in cases where a decision/measure must be taken urgently, the request is made to MASAK.

Case Study 2

As a result of the oversight activities carried out by IPRSA, it was determined that an insurance company transferred and registered shares without the permission of the IPRSA. In this regard, the insurance company was urgently requested to provide a defence on the matter. Also, despite the unauthorised nature of the transaction, information was requested from MASAK and relevant institutions regarding local and foreign legal and natural persons, as a share transfer was involved. In the statement made by the company, it was claimed that the share transfer in question was made mistakenly. In this context, the company was requested to delete the share transfer in question from the share register, restore the

entries in the share register to their previous state and submit the updated share register to IPRSA for approval.

Case 3

This case study comprises two separate applications reviewed by the CMB, with input from MASAK in the context of fit-and-proper and background assessments.

Case 3(a): Portfolio Management Company

An application was submitted to the CMB requesting authorisation to establish a portfolio management company ("A") with an initial capital of EURO 1.1 million within a registered capital ceiling of EURO 5.5 million. As part of the evaluation process, the CMB requested MASAK to provide information on any findings concerning the direct and indirect shareholders, as well as authorised representatives, of the proposed company.

MASAK conducted the necessary inquiries and shared its findings with the CMB. In addition, the opinion of the competent foreign authority was obtained in respect of an indirect legal entity shareholder exercising significant influence over the company. The assessments of both MASAK and the foreign authority did not reveal any adverse information and the application was assessed positively.

Case 3(b): VA Service Provider

Separate applications for establishment and/or operating licences relating to crypto asset service provider activities were submitted to the CMB. The CMB requested MASAK to assess the natural and legal persons included in the application against fit-and-proper criteria.

MASAK carried out the relevant checks and provided its findings to the CMB. For further details on the fit-and-proper assessment framework applied in this context, see IO3.

2.3.4. Customs and tax authorities

171. The MoT, Directorate General of Customs Enforcement (DGCE) adopts a structured and increasingly proactive approach to the use of outgoing international co-operation requests as a core operational tool in combating smuggling, predicate offences and associated financial crime. DGCE's authority to initiate international information exchange is established under Presidential Decree No. 1 and further operationalised through 72 bilateral Mutual Administrative Assistance Agreements, enabling systematic and lawful outbound co-operation with a wide range of foreign counterparts. CE authorities seek information through mutual administrative assistance and international operational co-operation to address all types of cross-border smuggling and trade-based risks. The DGCE co-operates with foreign counterparts and international organisations such as the WCO, Southeast European Law Enforcement Center (SELEC), and INTERPOL in order to determine potential risky routes related to smuggling and violations of customs regulations, including misdeclaration of origin and undervaluation; to identify high-risk consignments and related to persons, vehicles, and companies; trace criminal networks and facilitators; and co-ordinate simultaneous enforcement actions.

172. Statistical data indicates that there is regular and targeted use of outgoing co-operation mechanisms. In 2024, there were 65 outgoing information requests and 21 outgoing intelligence exchanges. In 2025, there were 116 outgoing information requests and 29 outgoing intelligence exchanges. Outgoing requests for information are primarily sent to support risk analysis and intelligence activities concerning seizures and suspicious persons and incidents. The feedback and intelligence outcomes obtained from international inquiries are carefully evaluated and can be utilised by the DGCE at the central level; furthermore, as deemed necessary based on the nature of the case, this information may be shared

with the relevant provincial customs administrations to be integrated into real-time risk analysis, targeting, and profiling operations.

173. Moreover, in combating cross-border crimes and various types of smuggling at both global and regional levels, the DGCE demonstrates a proactive approach. In this regard, successful outcomes are achieved through participation in international operations co-ordinated by organizations such as WCO, INTERPOL, and SELEC. Examples of such operations include EMPACT, THUNDER, DEMETER, PANGEA, PANDORA, TOX, GAMMA, WISE, Project Global Shield and STOP IV. Within the scope of the EMPACT operation co-ordinated by SELEC and conducted in October 2024, an operation targeting the smuggling of firearms, narcotics and commercial goods was carried out with the participation of EU Member States. During the operation, as a result of the risk analysis conducted by the DGCE, 120 kg of cocaine, migrants and undeclared goods were seized. Within the scope of the intelligence exchanges, controls carried out by the Customs Administrations of the United Kingdom, Greece, Portugal and Hungary regarding 10 suspicious shipments resulted in seizures with an approximate total value of EUR 26 400 000.

174. The tax authorities did not seek assistance from foreign counterparts during the period under review.

2.4. Providing other forms international co-operation for AML/CFT purposes, including asset recovery

2.4.1. FIU

175. Türkiye receives a large volume of international information requests relating to ML and associated crimes through multiple co-operation channels and Türkiye's international partners confirmed that Türkiye extensively provides quality non-MLA international co-operation. MASAK responds to a large number of incoming requests and provides spontaneous disclosures where relevant. LEAs, supervisory authorities and customs authorities similarly provide information and assistance through their respective channels.

176. MASAK prioritises incoming requests based on specific criteria. In this context, priority is given to requests in NRA reports regarding ML and TF threats at medium and higher risk levels, as well as requests involving vulnerable sectors and postponement of transactions, in addition to requests concerning customers, transactions and countries identified as high-risk by international organisations, particularly the FATF. Requests that are marked as "Very Urgent" and have a specific deadline are fulfilled separately from the matters mentioned above. Additionally, reminder emails are sent via EMIS before the deadline. Urgent requests are prioritised and fulfilled before routine or standard ones. Standard requests are typically responded to within 30 days in accordance with the Egmont Rules.

177. **Tables 2.11** and **2.12** capture incoming requests, all of which were addressed by MASAK and **Box 2.8** covers the postponement of a transaction and seizure of assets in addition to the outcomes of spontaneous disclosures made by Türkiye.

Table 2.11.: Number of Information Requests Received through Egmont Secure Web

Year	Incoming Requests	Spontaneous Requests	Total	Average Response Time (days)
2021	681	279	964	34
2022	715	198	946	47
2023	877	240	1124	49
2024	684	251	942	45
2025	574	201	775	34

Table 2.12.: Number of Incoming Financial Intelligence Exchanges with Other Non-Egmont Group Members

Requesting Countries	Years					
	2021	2022	2023	2024	2025	Total
East Asia				1	1	2
South Asia	1	3		1	1	6
Non-EU	3	30	7	5	20	65
Average Time of Response	18 days	46 days	55 days	71 days	23 days	

Box 2.8. Seeking of information by financial supervisors and Impact of submission of spontaneous disclosures

Case Study 1

In 2025, MASAK received a request from the FIU of Country X concerning suspected fraud against Bank Y involving EUR10.5 million, part of which had been transferred to three bank accounts held by Company Z in Türkiye. Following a request from the foreign authorities to postpone the transaction due to suspicions of fraud and ML, MASAK postponed the withdrawal of the EUR 382 000 held in one of Company Z's accounts, with the same quantum of funds subsequently seized.

Case Study 2

Country X was at different times spontaneously informed of certain suspicious actions that could form a fraud crime in line with Article 21 of ETS 30. Different suspects were accused of calling especially elderly and retired people living in Country X to convince them to invest in Türkiye and fraudulently taking their money. Eventually, this spontaneous information led to discovering the criminal organisation which was in charge of these crimes. Thanks to the dialogue between Türkiye and Country X, these spontaneous information sharing has resulted in the prosecution of fraud and the case is still ongoing.

2.4.2. Law enforcement agencies (LEAs)

178. The TNP receives and executes requests for information from foreign LEAs units. **Table 2.13.** sets out the number of information requests received by INTERPOL – Europol Directorate with an average response time of 2 to 8 weeks per year. **Box 2.4** contains an example of a joint investigation.

Table 2.13.: Number of Information Requests Received via Interpol Channel on ML Offence

Region	2021	2022	2023	2024	2025	Total
Central Europe	15	4	2	2	0	23
Southeast Europe	1	1	9	4	0	15
Western Europe	3	5	3	1	1	13
Northern Europe	2	4	3	0	0	9
Eastern Europe	5	3	1	1	0	10
Southern Europe	2	2	4	0	0	8

Middle East	0	0	1	1	1	3
Central Asia	0	0	2	1	0	3
Southeast Asia	3	0	0	0	0	3
Western Asia	0	0	0	0	1	1
South America	1	0	0	0	0	1
North Africa	1	0	0	0	0	1
East Africa	0	0	0	1	0	1
Grand Total	33	19	25	11	3	91

2.4.3. Supervisors of FIs, VASPs and DNFBPs

179. Supervisory authorities also play an important role in international co-operation. For the BRSA, the requests are generally related to fit and proper processes for opening overseas branches and appointing senior executives. For the IPRSA, the requests are generally related to identifying the beneficial owner of legal entities during the establishment phase and share transfer processes. For the CMB, the requests are generally related to fit and proper process. The CMB has not received any negative feedback regarding the coverage and timeliness of the information provided. If further information was required from the counterparty, in any case, there are open channels for bilateral dialog and any clarification. For the BRSA, information requests are prioritised and processed within a very short period of time. No negative feedback has been received from foreign counterparts regarding the contents of the information provided.

180. The CMB handled over 50 incoming requests from more than 25 jurisdictions during the period, responding to the vast majority of them, with average response times improving significantly from 82–94 days (2021–2023) to 41 days in 2025. The BRSA processed 68 requests from 2021–2025 with consistently short turnaround times (generally 10–27 days), reflecting efficient handling of supervisory co-operation. The IPRSA also engaged with a wide network of foreign supervisors, international organisations, and international bodies, exchanging regulatory and BO information as part of ongoing supervisory collaboration. Collectively, these figures demonstrate that Türkiye's supervisory authorities are not only recipients of international requests but also timely, reliable and proactive partners in addressing foreign authorities' information needs, including on legal and BO. IOSCO has a mechanism to follow the use of the IOSCO MoU by its members and assess its effectiveness. The statistics on the use of the mechanism by each signatory authority is collected every year by a dedicated international working group of IOSCO. Based on this mechanism, MMoU's effectiveness, the quality and the usefulness of the provided information and whether there is a discrepancy between members is checked and reported periodically.

2.4.4. Customs and tax authorities

181. Given Türkiye's strategic location and exposure to smuggling and transnational crime risks, international co-operation is an important component of CE's operational response. CE engages extensively in international information exchange to support risk analysis, intelligence development and operational enforcement against smuggling and related crimes. In 2023, CE conducted 129 formal information exchanges and 144 intelligence exchanges. In 2024, co-operation expanded significantly, with 195 incoming out of 260 information exchanges and 101 incoming out of 122 intelligence exchanges involving international organisations and partner countries. The high volume of incoming requests reflects both the importance of international co-operation in Türkiye's risk context and foreign reliance on CE's operational capabilities. Requests are prioritised according to subject matter and urgency and are generally addressed within one week to three months depending on complexity. While many intelligence exchanges are co-ordinated rapidly, more complex matters may require co-ordination across the General Directorate, provincial units, other Ministry units and external institutions. Information and document requests are supported through available databases, relevant sources and liaison channels, enabling a continuous flow of information that supports result-oriented risk analysis and operational action.

182. This co-operation supports investigations relating to hazardous waste, drugs, counterfeit medicines, wildlife, firearms, cultural property and high-value goods and has translated into co-ordinated enforcement outcomes. CE has participated in multinational operations including DEMETER 10, THUNDER 2024, PANGEA XVII, TOX, EMPACT, GAMMA and PANDORA IX targeting a broad range of transnational criminal activity. In 2025, CE processed 194 incoming information requests and 135 intelligence exchanges and participated in three international operations. Information exchange also contributed to concrete results, including arrests related to cigarette smuggling in various countries, particularly the United Kingdom and France. The consistently high volume of requests and demonstrated operational outcomes indicate that international co-operation is being used constructively to support disruption of transnational criminal activity.

183. Complementing this co-operation, the Turkish tax authorities play a substantive role in domestic and international co-operation supporting AML/CFT objectives. The Turkish Revenue Administration (TRA) and the TIB operate as complementary institutions with distinct functions, with the TRA serving as the competent authority for international exchange of tax information and the TIB contributing investigative expertise through audits and inspections. Through analysis of corporate structures, partnership relations and financial records, tax authorities contribute to identifying concealed ownership structures, entities misused for criminal purposes and laundering typologies. The TRA also functions as a designated channel for receipt and provision of beneficial ownership information to foreign counterparts, reinforcing Türkiye's capacity to support international investigations involving tax-related and ownership transparency concerns. The TRA has not received negative feedback regarding assistance provided.

184. Türkiye actively seeks and provides international co-operation for AML/CFT purposes through a wide range of channels used by the FIU, LEAs, supervisors, customs and tax authorities. Outgoing requests are generally aligned with the jurisdiction's risk profile and include financial intelligence, criminal intelligence and beneficial ownership information, with case examples demonstrating effective operational co-ordination and tangible asset restraint outcomes. Authorities also respond to a significant volume of incoming requests in a constructive and generally timely manner and international partners view Türkiye as a reliable counterpart. The volume of incoming requests, participation in multinational operations, demonstrated operational outcomes and complementary support provided by tax authorities indicate that co-operation is functioning effectively and broadly aligned with Türkiye's risk profile. While the number of outgoing asset-focused MLA requests remains modest relative to risk exposure and early freezing measures appear less consistently pursued in some cross-border asset recovery matters, these issues do not materially detract from otherwise effective co-operation outcomes. Overall, co-operation mechanisms appear stronger in providing co-operation and in seeking co-operation to investigate ML, TF and associated predicate offences, while further improvements remain possible in the more consistent pursuit of cross-border asset recovery.

3 Financial sector and virtual asset supervision and preventive measures

The relevant Immediate Outcomes considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this chapter are R.9-21, 26, 27, 34 and 35 and elements of R.1, 29 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Türkiye has established a comprehensive framework for the licensing of all FIs based on an effective two-tier licensing system. MASAK, as the main AML/CFT supervisor, and sectoral supervisors access a wide range of information to perform effective market entry controls to prevent criminals and their associates from entering the market. Authorities also conduct checks after the license has been granted as part of their supervisory activities. For VASPs, a solid regulatory framework has recently come into force but is still being implemented. All existing VASPs were required to reapply under the new framework and were operating under transitional arrangements, with licensing and fit-and-proper assessments still ongoing and not yet finalised at the time of the onsite visit, meaning that the framework had not yet become fully applicable to the existing VASP population. As none of the fit and proper assessments and VASP licensing processes had been finalised by the end of the on-site visit, the assessment team could not assess the effectiveness of the framework in practice.

b) Competent authorities demonstrated ability to detect unlicensed actors and the diverse methods employed to conduct their unlawful activities, supported by inter-agency co-operation and information exchange. Unlicensed MVTS are to a large extent detected and disrupted in line with Türkiye's risk profile. While cases where entities licensed for other activities (e.g. DPMS, foreign exchange or cargo operators) engage in unlicensed MVTS can be more complex and present more challenges, such cases are to at least some extent identified and acted upon through existing co-ordination and information-sharing mechanisms. Nevertheless, these mixed-activity cases highlight the importance of further strengthening co-operation among competent authorities.

c) Overall supervisors have a good understanding of ML/TF risks both at sectoral and entities level for FIs and VASPs. MASAK, as the main and primary AML/CFT supervisor, demonstrates strong

AML/CFT expertise within its Supervision of Obligations Department, whose staff show a deep understanding of ML/TF risks across different financial sectors, types of institutions, and emerging threats. With regard to VASPs, CMB's understanding of VASP-related ML/TF risks is still developing, in particular with regard to the technical specificities of VASP operations and the emerging risk profiles unique to the sector, as supervision of VASPs is a new responsibility for CMB. More broadly, compared to MASAK's Supervision of Obligations Department, sectoral supervisors, including CMB, demonstrate a less developed ML/TF risk understanding, with a greater focus on risk mitigation measures and, to a lesser extent, on the underlying and actual ML/TF risks themselves. This may affect their ability to carry out AML/CFT-related supervisory tasks effectively, including the conduct of AML/CFT inspections, and to ensure a balanced and effective supervisory framework.

d) FIs and VASPs have a generally strong understanding of the ML risks they are exposed to and the main ML risks identified by FIs and VASPs are generally in line with the findings of the NRA. Understanding of TF risks is more uneven. While banks (representing more than 75% of the sector) demonstrated a good understanding of TF risks, other FIs and VASPs have a more limited understanding, mainly considering TF risks in the scope of targeted financial sanctions. This uneven understanding contributes to challenges in TF detection and reporting, particularly in higher-risk sectors such as MVTS, exchange offices and VASPs. Authorities actively promote FIs' and VASPs' understanding of ML/TF risks through structured engagement mechanisms.

e) Overall, FIs and VASPs have a thorough knowledge of their AML/CFT obligations. Reporting entities apply mitigating measures, in particular CDD and take measures to identify beneficial owners. While the number of CDD deficiencies has decreased over the reporting period for most sectors, the incidence among exchange offices has remained high. FIs and VASPs also apply enhanced measures in relation to high-risk jurisdictions and scenarios. PEP identification and monitoring is only partially effective, particularly among Group B exchange offices, which represent a significant part of the sector and are typically smaller entities, Group B exchange offices are also not subject to a legal requirement to establish documented internal procedures. This structural feature affects the practical implementation of PEP-related and, more broadly, other AML/CFT obligations within this part of the sector. General reporting of suspicion from the highest risk sectors (banking, MVTS and VASPs) is substantial in ML cases, while it is low for other FIs. Overall, TF-related STR reporting remains limited across sectors, but is noticeably stronger in the banking sector than among other high-risk sectors. In particular, exchange offices, MVTS and VASPs show more constrained levels of TF reporting, suggesting challenges in TF detection and reporting relative to their assessed risk exposure.

f) Supervisors engage with FIs and VASPs through on site inspections, off site monitoring and case-based actions, using a combination of preventive, corrective and follow-up measures, applied according to entities' risk profiles. Türkiye's supervisory activities have an overall positive impact on compliance by FIs and VASPs. There is close and continuous communication between MASAK, sectoral supervisors and reporting entities, through frequent meetings, guidance documents, best practice papers and other outreach efforts on ML/TF. Across the board, reporting entities praise the quality of the relationship with their supervisors and provide tangible examples that supervisory activities, including the issuance of sanctions, had positive impact in supporting their compliance with AML/CFT requirements.

g) Supervisory authorities employ remedial actions to a large extent where breaches in compliance with obligations are detected. The adoption of the risk-based supervision approach in 2020 has led to a significant increase in the number of AML/CFT compliance supervisions, including both off-site and on-site supervisory actions, particularly on high-risk entities. Overall, enhanced supervisory actions have contributed to improved implementation of preventive obligations and greater awareness of AML/CFT requirements among FIs and VASPs. At the same time a relatively

high number of breaches continue to be identified through supervisory activities in certain sectors, notably exchange offices as well as among MVTS and VASPs, the latter showing observable improvements over time. Türkiye has also not sufficiently demonstrated that the most serious or systemic breaches have been appropriately addressed with sanctions that are proportionate and dissuasive. In addition, the absence of publication of AML/CFT sanctions and remedial measures further undermines their dissuasiveness and limits their preventive and deterrent effect across the FI and VASP sectors.

h) Enforcement remains heavily driven by the number of deficiencies identified during onsite inspections: administrative fines for CDD and STR breaches are imposed on a per-breach basis through fixed statutory amounts, with transaction-based minimum thresholds applying to most categories of FIs. This legal design limits the extent to which administrative fines can reflect the overall seriousness or scale of CDD and STR breaches. By contrast, even serious and extensive structural deficiencies — such as inadequate internal oversight and control, risk-management frameworks or the absence of institution-wide ML/TF risk assessments — are addressed through supervisory action that relies, in the first instance, on written warnings and a grace period for remediation. The sanctioning framework is formally graduated; however, as escalation is conditional on non-remediation and such deficiencies are typically remedied at the warning stage, they do not, in practice, lead to escalation to punitive sanctions in the absence of concurrent individual CDD or STR breaches. As a consequence, these systemic weaknesses — although often more serious in nature than individual CDD-/STR-related breaches — are not met with sanctions that are proportionate to their severity or sufficiently dissuasive. The supervisory response is not commensurate with the gravity and breadth of the deficiencies identified and does not provide a credible deterrent against future non-compliance.

Key Recommended Actions (KRAs)

Türkiye should:

d) Enhance FIs and VASPs understanding of TF risks and related mitigating measures, in line with a risk-based approach, with particular focus on high and medium-high risks sectors, such as VASPs, exchange offices and MVTS.

e) Enhance compliance with AML/CFT obligations, including, inter alia, suspicious reporting (including TF related aspects where relevant) and PEP obligations, in FIs and VASPs, following a risk-based approach, and enhance compliance with CDD requirements in exchange offices.

f) Ensure that the sanctioning and supervisory enforcement framework, including the use of remedial measures, is applied in a manner that strengthens the preventive and deterrent effect of enforcement. In particular, ensure that sanctions applied in cases involving more severe or systemic breaches of AML/CFT requirements are proportionate and sufficiently dissuasive, in line with the risk-based approach, including through a clearer calibration of sanctioning decisions to the seriousness and systemic nature of the breaches.

Other Recommended Actions

Türkiye should:

a) Enhance AML/CFT supervisory resources. This could be achieved either via enhancing MASAK's dedicated AML/CFT supervisory resources, and/or by strengthening the AML/CFT expertise of sectoral supervisors and other examiners involved in AML/CFT inspections, including through the allocation of dedicated staff within these institutions to conduct AML/CFT supervision.

b) Support further information sharing on ML/TF risks and enhance VASPs awareness of their AML/CFT obligations, this could be achieved through supporting the creation of a professional association.

c) Further enhance its ability to detect and disrupt unlicensed activities by continuing to strengthen co-operation and information exchange among LEAs, MASAK and sectoral supervisors.

d) Ensure that the competent authorities fully operationalise the VASP licensing processes and effectively implement the newly introduced regulatory framework, so that VASPs are subject to effective AML/CFT supervisory oversight in practice.

Overall Conclusions on IO.3

Türkiye has a comprehensive licensing framework to ensure criminals, and their associates are not beneficial owners or holding a management function in FIs. For VASPs, the newly introduced licensing framework had only recently entered into force and none of the licensing processes had been completed by the time of the onsite visit. As no VASP is yet required to comply with the strengthened requirements and all remain in a transitional phase, the effectiveness of the regime could not be demonstrated. Unlicensed activity is effectively detected and disrupted to a large extent, but challenges remain when already licensed entities perform money transfers for which they have not been licensed.

Overall supervisors have a good understanding of ML/TF risks both at sectoral and entity level for FIs and VASPs, which has translated into the implementation of risk-based supervision since 2020, supported by active supervisory engagement using a combination of on-site and off-site measures, as well as preventive, corrective and follow-up actions. High and medium-high risks sectors are prioritised and monitored more closely and high-risk entities in lower risk sectors have also been effectively supervised. Despite a significant increase since 2020, the AML/CFT expert resources within MASAK's Supervision of Obligations Department remain somewhat limited in light of its broad co-ordinating and oversight responsibilities across all sectors, while sectoral supervisors' ML/TF expertise is narrower, which affects the overall effectiveness of AML/CFT supervision.

Considering Türkiye's risk profile, the more limited understanding of TF risks by some higher risk sectors (exchange offices, MVTS and, to some extent VASPs) may lead to abuse of those sectors, even though they are not as commonly abused for TF as the banking sector, which is the predominantly abused sector for all TF risk factors. This concern is reflected in the NRA, which identifies TF cases where VASPs, MVTS and exchange offices have been abused by terrorist organisations and assesses VASPs as high risk and the MVTS and exchange office sectors as medium-high risk. The vulnerability of sectors varies depending on business models, transaction volumes and the nature of services offered. These risks are mitigated to some extent by the FIs and VASPs generally sound understanding of their AML/CFT obligations and application of mitigating measures accordingly, especially in the highest risk and more

material sector, namely the banking sector. This is consistent with supervisory actions undertaken in recent years, including measures implemented in the context of Türkiye's 2020 ICRG Action Plan, which have contributed to supporting FIs' and VASPs' understanding of ML/FT risks. However, this understanding does not always translate into consistent and effective implementation across all sectors, as illustrated by the exchange office sector, where the absence of a legal requirement for a large part of the sector to establish documented procedures limits the uniform and effective application of AML/CFT obligations, including enhanced measures.

Supervisory engagement and remedial actions have contributed to addressing a wide range of deficiencies at the FI and VASP entity levels. However, Türkiye has not demonstrated that the most serious or systemic breaches are addressed with sanctions that are proportionate and sufficiently dissuasive in practice. The current sanctioning approach, which places significant weight on the number of customer-level CDD and STR deficiencies while treating broader structural failures more leniently, does not provide a deterrent effect and limits the overall effectiveness of AML/CFT supervision. In addition, the lack of public disclosure of enforcement actions further limits their preventive and deterrent effect across the financial sector.

Despite the identified strengths, the assessment placed particular emphasis on the deficiencies highlighted in the Key Recommended Actions, which address distinct and substantive weaknesses in the supervisory framework that require major improvements to be addressed effectively.

Türkiye is rated as having a Moderate level of effectiveness for IO.3.

Immediate Outcome 3

185. MASAK is the AML/CFT supervisor in Türkiye, meaning that it oversees compliance with ML/TF obligations for all reporting entities. Beyond MASAK, there are five sectoral supervisors for FIs and VASPs, overseeing compliance with all other obligations. BRSA supervises banks, factoring/financing/leasing and asset management companies. CMB supervises the capital market sector and VASPs. CBRT supervises MVTS. IPSRA supervises insurance companies. General Directorate of Financial Markets and Foreign Exchange (GDFMFE) and TCB (both from MoTF) regulate and supervise exchange offices and precious metals intermediaries respectively.

186. MASAK and sectoral supervisors' roles are complementary. MASAK oversees Türkiye's AML/CFT supervision plans, it can conduct onsite/off-site inspections or mandate sectoral supervisors or other authorised examiners. If during the course of its prudential inspection, a sectoral supervisor detects an AML/CFT breach, the case is referred to MASAK for further inquiry and potential issuance of sanction.

187. In assessing the effectiveness of Türkiye's supervision of FIs and VASPs, the AT placed the most weight on the banking sector, given its materiality (representing more than 75% of Türkiye's financial sector). It also placed significant weight on VASPs, exchange offices and MVTS given the high risks they present in line with the findings of Türkiye's NRA and due to the potential abuse of those sectors especially for TF purposes considering Türkiye's particular context.

3.1. Licensing, registration and controls for FIs and VASPs preventing criminals and associates from entering the market

3.1.1. Market entry controls

188. Türkiye has established a comprehensive framework for the licensing of all FIs based on an effective multi-tier licensing system. MASAK, as the main AML/CFT supervisor, and sectoral supervisors access a wide range of information to perform effective market entry controls to prevent criminals and their associates from entering the market. Authorities also conduct checks after the license has been granted as part of their supervisory activities. For VASPs, a solid regulatory framework has recently come into force but is still being implemented. Fit-and-proper checks were at an advanced stage at the time of the onsite, but had not yet been completed.

189. Market entry controls are carried out by sectoral supervisor for each relevant sector. All FIs and VASPs are required to be licensed and registered by competent authorities through a multiple stages licensing process consisting of two main steps: an establishment permit and an operating permit.

190. During the establishment phase, FIs must be established as joint-stock companies, with contracts of incorporation, and they must meet certain conditions such as capital requirement. Fit & proper requirements also apply to the founding partners, shareholders above 10% or persons having ultimate control over the FI, which require that those individuals should not have been convicted of any crime including those related to capital market and have sufficient financial strength and professional competency. The shareholding structure is required to be transparent and as joint-stock companies, FIs are required to file their BO information to the TRA.

191. In most cases, this initial phase includes a physical meeting between the sectoral supervisor and the applicant, allowing to further inquire on fit and proper requirements as well as better understand the objectives and business model of the applicant. In cases where the conditions, qualifications and competencies required for obtaining the permits are not met, applications are halted at this initial stage, including if founding partners, ownership structures or business model are deemed unsuitable. Most rejections of applications happen at this initial stage, with candidates also withdrawing their applications before a negative decision is made.

192. The licensing process is supported by extensive inter-agency co-operation. Supervisors obtain information from multiple sources (open-source media, sanctions screening) and there is strong co-operation with other competent authorities to access more sensitive information (criminal records, etc). When needed, additional information is also requested to foreign competent authorities, particularly in relation to foreign ownership applications. Sectoral supervisors obtain BO information indirectly through the TRA or other competent authorities, whereas MASAK and the TIB have direct access to the BO Registry. The TIB may also carry out AML/CFT supervisory tasks, in addition to its tax inspection activities. The supervisors demonstrated a sound understanding of the concept of BO taking into consideration that a partner owing less than 10% of the share could actually be the BO via appointment rights of privileged shares.

193. Based on its licensing process, Türkiye has a high level of rejection of applications in all FIs sectors with the exception of the banking sector. Authorities explain that this is due to the thoroughness of the establishment permit phase especially for banks, where applicants prefer to withdraw their applications if shortcomings are identified at this early stage. The high number of rejections in the EO sector is explained by a legislative change in 2024 leading to enhanced requirements, as this led authorities to reject all applications in the sector for this year and reconsidering them the following year. For precious metal intermediaries, financial liability shortcomings is the main reason for rejecting licenses.

Table 3.1. Licensing of FIs and VASPs (2020-2025)

Institutions	Approved	Rejected	Cancelled / Suspended	Overall number of FIs
Banks	33	0	1	63
Non-Bank Financial Institution (NBFIs)	60	21	21	124
MVTS	42	15	7	89
Capital Market Sector	115	46	4	205
VASPs	98	76	0	58
Insurance	31	20	6	73
EO	94	123	41	773
Precious Metals Intermediary	33	74	24	46

194. VASPs were brought within the scope of obliged entities under the AML/CFT framework in 2021. However, it was not until March 2025, that Türkiye established a robust licensing process for VASPs, similar as for other FIs. Before that, there were no comprehensive entry controls, including fit-and-proper and ownership checks. At the time of the on-site visit, the fit-and-proper assessments were well advanced but had not yet been finalised; moreover, the broader licensing process, including other entry controls, was still ongoing. As none of the fit and proper assessments had been finalised and no VASP licences had been granted by the end of the on-site visit, the assessment team could not assess its effectiveness at that stage. CMB is applying enhanced measures at market entry due to the high ML/TF risks associated with VASPs in Türkiye. All VASPs willing to continue operating in Türkiye had to reapply by mid-2025 in line with the newly introduced requirements. Consequently, none of the VASPs is yet obliged to comply with the new, stricter regulatory framework. Those that did not reapply will have to cease their activities by the end of 2025 while the remaining ones have been granted a transition period to comply with the new requirements by June 2026. As a result, the overall number of VASPs operating in Türkiye has already decreased from 88 in 2024 to 58 currently, all waiting to be licensed. All foreign VASPs willing to operate in Türkiye must establish a branch or subsidiary that is subject to the fit and proper requirements described above. Foreign legal and natural persons involved in the ownership or management structure of a VASP are subject to stringent controls. The CMB built upon its experience of licensing capital intermediaries' institutions to initiate the licensing process to VASPs while ensuring its staff and procedures were adapted to the challenges brought by those new actors. In addition to fit and proper requirements on founders and managers, CMB supervisors are supported by specialists from Türkiye's national scientific and technologic agency (TUBITAK) to test the IT systems before delivering the operational permit.

195. Sectoral supervisors maintain active monitoring of fit and proper requirements following the licensing process. This ongoing monitoring also applies to VASPs after the completion of the licensing process and the granting of a licence. By law, any change in the ownership structure involving 10% or more of the share has to be declared to the supervisor. The partnership and ownership structures are also part of the elements review during the supervision activities conducted by both prudential supervisors and MASAK in the scope of its AML/CFT monitoring activities. Sectoral supervisors can also attend annual FIs board meeting. In the EO sector, monitoring is applied to newly licensed entities after 90 days. Entities have to provide camera footage for the GDFMFE to review if the activity is indeed conducted by the individuals declared as holding management functions.

Box 3.1. Fit & proper requirements case studies

Case 1 - BO: In 2020, an investigation was conducted into a company owned by two individuals named X and Y on suspicion of unauthorised activity, and it was determined that this company was providing unauthorised payment services. A complaint was filed with the Chief Public Prosecutor's Office against the company and its shareholders, and legal proceedings were initiated. While the legal proceedings

were ongoing, in 2021, during an application for an activity licence, it was determined that the applicant company had a sole shareholder, whose spouse was X, and that one of the companies from which the applicant company planned to receive services was another company owned by Y. The application was rejected on the grounds that the shareholder of the applicant company was not the beneficial owner and that his spouse, X, and Y were acting fraudulently to conceal the beneficial owner.

Case 2 – Foreign individual: A foreign national, Mr. A submitted an application to the Capital Markets Board requesting a licence to establish an intermediary institution under the trade name "XXX A.Ş." It was envisaged that the company to be established would have a capital of approx. EUR 10M and that all of its shares (100%) would be owned by Mr. A. In the scope of the examination of the application, opinions were obtained from other public institutions. The Ministry of Foreign Affairs reported that Mr. A was a political figure with tied relation in Country A and that he had contacts with persons considered as terrorists by Country B, and that he was involved in smuggling oil smuggling through fake contracts. BRSA also stated that Mr. A was a founding partner of an asset management company and the operating licence of that company was revoked on the grounds that Mr. A had lost the founding conditions. Taking this into account, it was concluded that MR A did not meet the fit and proper requirements and therefore the license to establish XXX A.Ş. was rejected by CMB.

Case 3 – monitoring requirements: The CMB filed a criminal complaint against Mr. E for "improper public offer and unauthorised capital market activity" (Law 6362, art. 109/2). Mr. E, an indirect shareholder of Investment Firm YYY A.Ş. and also chairman of its board of directors, holds 100% of the shares in BBB Investment Holding A.Ş., through which he indirectly owns 100% of YYY A.Ş. Following his conviction, Mr. E lost the condition that founding partners must not have a final conviction for the offences specified in the CMB Law. Therefore, the CMB took a measure regarding both the shareholding structure (granting the investment firm a 3-month period to ensure that Mr. E's indirect shares were transferred to persons who meet the legal requirements) and the board membership (removing Mr. E from his position as a member of the board of directors of Investment Firm YYY A.Ş).

3.1.2. Detecting and addressing breaches

196. Türkiye detects unlicensed FIs activities to a large extent and measures are taken when those are identified. Overall, authorities demonstrated a co-ordinated approach combining preventive, supervisory, and enforcement actions, contributing positively to the effectiveness in detecting unlicensed activities. Identification is allowed through various channels such as denunciation mechanisms open to public, LEAs, tax inspections, notifications from other supervisory authorities and social media monitoring.

197. After their detection, persons engaging in unlicensed activities are sanctioned in accordance with the respective legislation, either leading to administrative sanctions or to judicial proceedings depending on the qualification of the offence (see below table). Acting as an FI without a licence is an offence, but some cases relate more to fraud than carrying out unlicensed FI activity. Supervisory authorities are also entitled to act accordingly to stop the unlicensed activity and deliver administrative fines.

Table 3.2. Judicial actions undertaken for unlicensed activities (2020 – 2025)

Institutions	Investigations		Prosecutions		Convictions	
	Files	Persons	Files	Persons	Files	Persons
Banks	183	282	85	126	8	10
NBFIs	43	88	19	45	8	26
MVTSs	1 301	2 732	653	1 166	169	248
Capital Market Sector	439	1 247	74	305	70	106
Insurance	159	222	42	66	10	12

198. CMB established a dedicated unit in charge of monitoring VASPs licensing as well as examining complaints received from the public on illegal activities. So far, 132 complaints have been processed leading to the referral of 10 actors to the PPO. By the end of the onsite, no sanctions had been imposed against unlicensed VASP activities. However, CMB also blocks access to the websites of unlicensed VASPs, which forms part of its efforts to prevent illegal operations. Due to VASPs being a newly supervised entities, CMB, is still developing its understanding of VASPs business models, operational techniques, and risk profiles. This learning curve may affect the ability to fully identify unlicensed VASPs activities and emerging risks. Strengthening co-operation with LEAs and other competent authorities would further enhance detection capabilities and support effective enforcement.

199. Authorities have identified and taken remedial actions against unlicensed MVTS to a large extent with a significant increase in the number of cases detected, investigated and prosecuted over the reporting period. This highlights enhanced efforts by competent authorities to address unlicensed MVTS activities, including hawala– illegal in Türkiye- which have been resorted to in ML/TF cases in Türkiye (see IO.7). However, gaps remain in identifying the full scope of such unlicensed operators. In particular, authorities may not consistently recognise cases where entities licensed for other activities (e.g., as DPMS or cargo operators) also engage in unlicensed MVTS. Information collected by other authorities about these mixed-activity entities is also not always effectively shared with CBRT, which may impact its ability to fully detect unlicensed actors.

200. As mentioned above, authorities strengthened in 2024 their requirements for licensing and monitoring exchange offices. More than 100 companies were asked to submit camera footage to verify operations and detect wrong doings. This process, that will be repeated annually, has led to an enhanced detection of wrongdoings of exchange offices in 2025 and the allocation of fines.

Table 3.3. Actions undertaken against unlicensed exchange offices

Year	Closure of workplace		Total amount of admin fine (EUR)
	Temporary	Permanent	
2021	53	19	204 000
2022	97	23	192 000
2023	72	23	336 000
2024	145	48	1 163 000
2025*	116	18	480 000
Total	**483**	**131**	**2 375 000**

Note: *until November 2025.

Box 3.2. Unlicensed activities cases study

Case 1: BRSA received information through various channels, alleging that a company established in Country A under the name XXX Bank is providing banking services by claiming to be a branch of a bank in Istanbul, posting information and announcements on its website, making efforts to acquire customers, and issuing a letter of guarantee. First, the relevant counterpart authority in Country A was contacted to request information on whether there was a bank operating under this name in their country, and it was confirmed that no such bank was established. As it was determined that the activities of XXX Bank could constitute the "crime of unauthorised activity", BRSA submitted the case to the PPO, also requesting to suspend the activities, advertisements, website, and, if applicable, the operations of any branches of XXX Bank, and block access to its website. This was obtained and the prosecution regarding the case is ongoing.

Case 2: In a complaint/notification submitted to CMB through the Presidential Communication Center, it was alleged that virtual asset service provider activities were being conducted through a website ABCD. In this case, it was found that activities of the website ABCD were directed towards persons resident in Türkiye while ABCD did not have any established activity in the country as required by law. The necessary legal procedures for blocking access to the ABCD were undertaken. In addition, during the review of the website ABCD, it has also been determined that the domain name service provider was acquired by an individual named X. When approached by authorities, X claimed that individuals were using his identity to conduct their illegal activities which was confirmed following further investigation. Upon reviewing the payment information related to the purchase of the ABCD domain, it was determined that the payment had not been made by X, but instead by two individuals named YY and ZZ who are currently under investigation.

3.2. Supervisors identifying understanding and promoting FI and VASP understanding of ML/TF risks

3.2.1. Identifying and maintaining an understanding of the ML/TF risks in the different sectors and types of FIs and VASPs and of individual FIs and VASPs over time

201. Supervisors generally have a good understanding of ML/TF risks both at sectoral and entities level for FIs and VASPs. The AML/CFT expert resources within MASAK's Supervision of Obligations Department demonstrates a deep understanding of ML/TF risks across different financial sectors, types of institutions, and emerging threats. By contrast, sectoral supervisors risk understanding is less developed and focuses more on risk mitigation measures and, to a lesser extent, on the underlying and actual ML/TF risks themselves. Given MASAK's role as the primary AML/CFT supervisor, this difference in understanding is expected; however, enhancing sectoral supervisors' knowledge of ML/TF risks would strengthen the effectiveness of their AML-related supervisory activities.

202. In 2021, as part of its AML/CFT Strategy, Türkiye established the "Threat and Vulnerability Working Groups", led by MASAK and comprising all relevant competent authorities, in charge of assessing Türkiye's ML/TF risks. Under the Vulnerability Working Group (WGs), 8 risk analysis sub-groups were created to assess sectoral risks and entities risk level for banks, NBFIs, capital markets, MVTS, insurance, EO, VASPs and DNFBPs. Under the supervision of MASAK, those sub-groups are gathering sectoral regulatory and supervisory authorities, professional associations of each sector and representatives of the private sector.

203. In 2022, the Risk Analysis WGs first determined and evaluated the inherent risks of the sectors and calculated residual risk scores, considering mitigating measures applied by the obliged entities. The general method used in the risk analysis of the financial sector is comprised of 4 phases. In the first phase, inherent risks of the sectors are identified and assessed by taking the impact and likelihood of the risks. In the second phase, measures used by the sectors to mitigate the inherent are identified and assessed to determine their effects. This leads to the third phase where a survey is sent to reporting entities in each sector to determine which of the risk mitigating measures (among the ones identified in the second phase) they are using to manage their risks. As a result, residual risk scores for each obliged party is calculated by assessing the measures they are taking. In the fourth phase, risk factors that are not included in the first three phases but that are important for risk analysis are included in the analysis. Those criteria consist of size of the sector, results of supervision of AML/CFT and prudential obligations, materiality (transaction volume, asset size etc.), STRs, analyses report from MASAK, and other notifications/denunciations sent about the reporting entities. All those factors are considered, and the sectoral risk level is identified and assessed annually.

204. Türkiye has established a similar, multi-phased methodology to assess ML/TF risks at the level of individual FIs and VASPs (entity level risk scoring), updated yearly which serves as a basis for the implementation of risk-based supervisory programmes (see 3.5). The methodology combines inherent risk analysis, evaluation of mitigating measures, and integration of supervisory and enforcement data to produce a comprehensive risk profile for each entity. Consultation with the private sector is ensured though professional associations. For the EO sector, while there is no professional association for which the membership is mandatory, consultation was conducted through the Risk Analysis WGs for EOs, which includes participation from private sector representatives. For VASPs, consultation occurs through the Türkiye Capital Markets Association (TCMA), as there is no professional association dedicated solely to VASPs. Each entity is categorized into one of three risk categories (high, medium, low) based on their overall net rating. Entities' individual rating is reviewed annually for all FIs and VASPs.

Table 3.4. FIs and VASP risk level

Institutions	Sectoral risk level	Overall number of Institutions	2024 Entities Risk Level (number)	
			High	Medium
Banks	High	63	3	28
VASPs*	High	88	5	33
MVTs	Medium High	89	5	35
Exchange Offices	Medium High	773	35	129
Capital Market Sector	Medium	205	10	42
NBFIs	Medium	124	6	36
Insurance	Medium Low	73	2	0
Precious Metals Intermediary	Medium Low	46	2	0

Note: * the figures presented for VASPs are before the introduction of the 2025 licensing process that was still ongoing at the time of the onsite visit.

205. The distribution of entity-level ratings indicates that only a small proportion of institutions within each financial sector are classified as high risk - approximately 5–6% even in sectors assessed as having high or medium-high inherent risk (banks, VASPs, MVTS providers and EOs). This does not, in itself, indicate misclassification of risk at entity level, as sector-level risk does not imply that all entities within the sector present the same risk profile, and entity-level risk assessments appropriately reflect differences in size, products, services and exposure. Nevertheless, the limited number of entities classified as high risk may suggest that the current scoring methodology does not fully capture variations in risk across the FI and VASP population. As outlined in section 3.5, Türkiye's supervisory authorities direct supervisory attention not only to high-risk but also to medium-risk institutions. In this context, while the small number of entities

classified as high risk should be noted, the assessment of how supervisory resources are applied proportionately across different risk levels is even more important. The risk categorisation is ultimately a tool to guide supervisory prioritisation, rather than an objective in itself.

206. MASAK has undertaken significant efforts to build an understanding of ML/TF risks in the VASP sector through a strategic analysis in 2022, updated in 2025. The updated study involved data collection on 74 VASPs, including transaction patterns, customer activity, banking relationships, STRs, adverse media, and enforcement records. This analysis concluded that VASPs pose high ML/TF risks, driven by factors such as sector size, product diversity, high violation rates, and confirmed cases of misuse for fraud, illegal betting, gambling, drug trafficking, forgery, and TF linked to terrorist organisations exploiting religious beliefs. These findings demonstrate that MASAK has a strong grasp of sectoral vulnerabilities and emerging risks. CMB's understanding of VASP-related ML/TF risks is still developing, in particular with regard to the technical specificities of VASP operations and the emerging risk profiles unique to the sector, as supervision of VASPs is a new responsibility for CMB. While CMB has longstanding experience in licensing and supervising capital market actors its awareness of VASP-specific risks is less developed than MASAK's, indicating uneven understanding across competent authorities.

207. In general, sectoral supervisors' understanding focuses more on risk mitigation measures and, to a lesser extent, on comprehensive understanding of the actual ML/TF risks their sectors are exposed to. This could explain why sectoral supervisors - whose primary focus is on prudential supervision - despite participating in the risk working groups, articulate the actual ML/TF risks their sector is exposed to less comprehensively than MASAK. While this is to some extent aligned with the role they play in the system, strengthening their understanding would significantly enhance their effectiveness, particularly as they form part of MASAK's AML/CFT supervisory strategy.

3.2.2. Promoting FI and VASP understanding of ML/TF risks and AML/CFT obligations

208. Authorities actively promote FIs' and VASPs' understanding of ML/TF risks through structured engagement mechanisms. As described above, the Threat & Vulnerability WG and the sectoral risks working groups provide a platform for FIs and VASPs to share their perspectives on emerging risks and, in turn, to gain insight into the supervisors' risk assessments and supervisory priorities. These forums not only facilitate dialogue but also contribute directly to the development of the sectoral risk assessments which feed the NRA and of supervisory programs (see 3.5).

209. Findings from Risk Analysis WGs have informed the preparation of Sectoral Risk Assessment Reports by professional associations, ensuring that sector-specific vulnerabilities are clearly identified and communicated. However, such reports have not been prepared for some high/medium-high risk sectors (e.g. VASPs and exchange offices). This is largely due to the absence of a dedicated professional association for these sectors. While the Türkiye TCMA participated in the Risk Analysis Working Group for VASPs, it is not an association exclusively established for VASPs. During the onsite visit, VASP representatives emphasized the need to create a dedicated professional association to further promote understanding and information sharing on ML/TF risks.

210. MASAK's activities have strengthened FIs' understanding of ML/TF risks and their related obligations to a large extent, with financial institutions widely acknowledging the quality of the work conducted by MASAK. Over the reporting period, and in line with the requirement of the ICRG Action Plan, MASAK has conducted a significant number of trainings and workshops for all FIs and VASPs.

211. MASAK also provides feedback to FIs and VASPs relating to their AML/CFT supervision results and publishes guidelines on ML/TF risks and AML/CFT obligations. This collaborative approach enhances transparency and supports FIs in aligning their risk management frameworks with national priorities. This is an ongoing work, as a result of the 2025 NRA, more than 10 guidance documents are being updated

including on STRs, ML/TF typologies, PEP, VASPs, BO, identification of parties to a trust agreement established abroad. FIs met during the onsite were also keen on receiving more general feedback on the overall results of supervision in their respective sector.

3.3. FI and VASP understanding of existing and evolving ML/TF risks

212. FIs and VASPs met during the onsite visit have a generally strong understanding of the ML risks they are exposed to. The main identified ML threats for the highest risk sectors (banks, VASPS, and MVTS, and to a lesser extent exchange offices) are in line with the main predicate offences of the NRA, namely fraud, illegal betting and gambling. Understanding of TF risks is more uneven, while banks (representing more than 75% of the sector) have a good understanding, other FIs and VASPs have a more limited understanding, mainly considering TF risks in the scope of targeted financial sanctions. Also, the low levels of TF STR reporting across several other higher-risk sectors - particularly MVTS, exchange offices, and VASPs - indicate an uneven understanding of TF risks.

213. Representatives of the Turkish banking sector met during the onsite demonstrated a good understanding of specific ML/TF risks their institution is exposed to, as well as related mitigation measures. This understanding has been supported by the work conducted by the Risk Analysis WG, gathering competent authorities and representatives of the private sector (see above) including the banks association of Türkiye. The WG identified inherent risks across almost forty distinct products and services and the related mitigated measures adopted by banks. This also supports the implementation of a risk-based approach by banks, while higher-risk products (e.g., third-party payments, cardless transactions, banking services for VASPs and payment institutions) receive more intensive measures, lower-risk are subject to fewer controls.

214. VASPs met during the onsite despite their more recent entry in the market, also demonstrated an overall solid understanding of their ML risks. There was some variation in the depth of understanding, with larger and more established entities demonstrating a more comprehensive grasp compared to smaller and recently established ones. The differences were more pronounced for TF risks, with the larger entity identifying those while others having a much more limited understanding, which is somehow concerning, considering the sector high exposure.

215. Among other FIs, understanding of ML risks is uneven. Across sector, larger institutions generally have a deeper understanding of these risks while others focus on risk mitigation measures rather than the inherent risks their sector and institution are exposed to. The fact that all institutions were able to describe risk mitigation measures indicates a general awareness of ML threats even if not always articulated as such by FIs representatives.

216. The understanding of TF risk among FIs – except for banks - is more limited and mainly considered within the scope of targeted financial sanctions. Banks, which represent the largest and most materially significant part of the financial system, demonstrated a generally more developed understanding of TF risks. This is more concerning for MVTS and exchange offices. While TF risk exposure may vary across entities depending on size, business models and products offered, TF-related vulnerabilities identified in these sectors in Türkiye's context, and the uneven understanding of TF risks observed during on-site discussions, increase their susceptibility to misuse. This concern is further supported by the NRA, which recognises TF risks in both the exchange office and MVTS sectors, including cases where terrorist organisations have abused these sectors. Competent authorities indicated that, while such cases exist, they are limited in number. MASAK has undertaken a range of initiatives in recent years to strengthen the private sector's understanding of TF risks—including workshops, updated guidance documents and TF typologies. However, these measures have not yet translated into a corresponding improvement in the practical understanding of TF risks among FIs, except for banks, and some larger VASPs.

3.4. FI and VASP understanding and compliance with AML/CFT obligations and mitigating measures

3.4.1. CDD, record-keeping, BO information, ongoing monitoring

217. Generally, FIs and VASPs have effective processes in place for onboarding customers and applying CDD supported by electronical automated system. CDD are performed regularly, the frequency of customer profile's review follows a RBA. It is typically conducted every year for high risks clients, every two to three years for medium risks and every four to five years for lower risks clients. Those reviews are often supported by the use of electronical tool including artificial intelligence (AI), allowing for a modular approach taking into account several risk parameters at the same time: client risk profile but also typologies of transactions or specific jurisdictions. Those tools allow entities to adapt their monitoring by taking into consideration a wide range of indicators, analyse cross-cutting data to cope with emerging and evolving risks and also identify triggering scenarios even for lower risk customers.

218. Certain sectors, specifically exchange offices, MVTS, and VASPs, have a higher incidence of CDD deficiencies compared to banks and other FIs. While the number of CDD deficiencies has decreased over the reporting period for most sectors, a continued identification of a high number of breaches has been observed among exchange offices.

219. VASPs mostly resort to virtual know your customer (KYC) procedures for onboarding natural persons or Turkish nationals, depending on institutional policy, while in-person onboarding process are conducted for legal persons and/or foreigners. On average, VASP report a low number of clients being legal entities. New customers also have to make their initial deposit via a bank account transfer which allows for further monitoring of their profile.

220. FIs and VASPs demonstrated their general ability to check BO information by resorting to a range of information sources and supported by digital tools. All FIs and VASPs acknowledged challenges in verifying BO information in complex structures but were able to explain the verification sources and channels used. Some FIs, especially banks and VASPs, reported the use of in-house AI program to check BO information, particularly for shareholders below the 10% partnership threshold and when foreign partners are involved. FIs and VASPs do not have direct access to the BO Registry. Instead, they request their customers to provide a QR code that grants access to the customers' BO information in the BO R registry. Customers also have an obligation to declare any transaction they would conduct on behalf of someone else, and FIs and VASPs apply enhanced monitoring in those cases with some rejecting such activity. Overall, FIs and VASPs demonstrated a sound understanding of basic beneficial ownership concepts. However, while banks exhibit a more developed and structured appreciation of risks linked to foreign-created legal persons and foreign legal arrangements, there was variation in the ability of some other FIs and VASPs to describe the measures they take to fulfil their CDD and BO obligations in multi-jurisdictional ownership chains and in more complex interactions involving foreign legal persons, including legal arrangements which do not exist domestically. Such variation may indicate limitations in risk understanding, which in turn may affect the consistency and robustness of the mitigation measures applied.

221. The AT was also made aware of a case in which supervisory authorities identified significant deficiencies regarding a VASP in the context of supervisory activities. In this case, the VASP lacked any real-time, periodic or automated monitoring, and had no processes to assess whether customer transactions were consistent with the customer's professional or economic profile. While the VASP addressed the deficiencies identified through supervisory action, this individual case indicates that there may be substantial differences in compliance within the VASP sector. This is particularly relevant in light of the transitional period granted for the implementation of the more stringent regulatory requirements

applicable to VASPs and the fact that supervision under the new more stringent regulatory framework has not yet been conducted.

222. Reliance on third party is resorted to a limited extent, mostly by FIs with a broader international remit who take advantage of institutional capacities especially when identifying or verifying foreign customer, for CDD and BO.

223. Record keeping requirements are overall understood and applied, especially with the use of digital tools. Failure to comply with record keeping requirements is an offence in Türkiye, supervisors have filled 11 criminal complaints against FIs and VASPs for such shortcomings over the reporting period.

3.4.2. Enhanced or specific measures

224. Most FIs and VASPs have procedures for identifying PEPs, but compliance with this obligation is relatively recent (2022) and remains challenging to some extent. However, as noted in the previous MER (2019, KF c)), FIs had already applied EDD measures to PEPs, their family members and close associates prior to 2022, although these measures were not considered comprehensive at the time. FIs and VASPs ask customers about their principal occupation or employment and resort to commercial databases and open sources information to identify PEPs and their relatives. Those tools present limitation especially in the identification of PEPs closes relatives and associates and none of the entity met onsite reported to directly ask their customer whether they are considered as a PEP or a relative. In addition, some FIs have limited awareness that close associates include not only relatives but also individuals with social or professional ties to a PEP. Main FIs and VASPs, especially those belonging to international groups, demonstrate a better ability to detect PEPs, including foreign ones.

225. However, only half of the EOs declared to have procedures for identifying PEPs, which severely impacts the sector's ability to identify PEPs. This is to a large extent explained by the regulatory framework, under which Group B exchange offices - which constitute approximately 78% of all EOs and are typically smaller entities - are not required to establish formal written procedures. However, the absence of a legal requirement for Group B Eos to establish formalised, documented procedures for identifying and reviewing PEPs, combined with the fact that in practice only around half of all exchange offices have such procedures, significantly weakens the sector's overall capacity to comply with PEP-related obligations. Although the exclusive compliance officers appointed by Group B exchange offices carry out risk management, monitoring and control activities to some extent even without clear written procedures, the lack of documented and standardised processes means that there is no assurance that Group B exchange offices can consistently detect higher-risk customers or comply reliably with EDD requirements (including PEP-related requirements). Without clear and documented procedures, it cannot be ensured that EDD obligations are implemented effectively and uniformly across Group B exchange offices.

226. While a limited number of other FIs and VASPs do not have clear procedures for the identification and review of PEPs, discussions held during the onsite visit indicated limitations in the practical identification of PEP customers by some of the entities met. This points to shortcomings in the effectiveness of PEP identification measures in practice. While MASAK's PEP guidance outlines methods to identify PEPs, family members, and close associates, it does not provide examples of prominent public functions considered PEPs in Türkiye.

227. Banks have a good understanding and take appropriate mitigating measures in relation to correspondent banking relationship. They have an institutional policy defining how to operate and high-risk jurisdictions and entities defined at the group level. Even though those policies can differ among financial institutions, they include high-risk jurisdictions as identified by the FATF. There is also an automated monitoring of open-source information monitoring potential adverse media reports, allowing to take appropriate measures as needed towards identified entities. Banks widely reported the systematic

involvement of compliance units for transactions with entities located in high-risk jurisdictions or entities considered as presenting a higher risk. None of the banks met during the onsite offered payable-through accounts.

228. Banks and MVTSs are also taking enhanced measures to monitor the use of higher risk products such as prepaid card services. Entities run scenario alerts daily, monthly and quarterly, and review their criteria on an ongoing basis to monitor such products with the implementation of EDD measures.

229. Despite the recent implementation of travel rule obligations in Türkiye (December 2024), VASPs met during the onsite demonstrated a strong understanding of those requirements. Certain VASPs reported to have their own institutional policy which goes beyond legal requirements and to refuse transfers with entities that do not comply with the travel rule requirements. VASPs also compel clients' declaration regarding the beneficiary/originator of the VA transfer and trace transactions through blockchain analytic tools. TUBITAK is currently developing tools to support VASPs complying with travel rule obligations and VASPs met during the onsite highlighted the positive expected impact of such initiative. Enhanced controls are applied to transactions involving hot wallets connected to certain jurisdictions. In these cases, the transaction is automatically flagged and the entity must complete an additional step to validate it. VASPs reported that transactions involving mixers or unhosted wallets are generally not accepted and returned to the originator There is also a daily withdrawal threshold of approx. EUR 2 500 and a monthly threshold of EUR 42 000 allowing to amount transferred.

230. FIs and VASPs have also adopted specific measures to address risks arising from new technologies. The implementation of controls for new technologies is particularly strong among highest risk sectors.

3.4.3. AML/CFT reporting obligations, tipping off

231. Overall, FIs and VASPs have a general sound understanding of their STRs obligations. Between 2020 and 2024, suspicious transaction reporting has significantly increased by approximately 130%, with all sectors increasing their reporting demonstrating an enhanced compliance over the reporting period. In 2024, 98% of STRs were submitted by banks, MVTS and VASPs, which is in line with those sectors risk profile. EOs, assessed as presenting medium-high risk, reported a marked increase in STRs between 2020 and 2024 (approximately 115%), with volumes peaking in 2023. Nevertheless, in 2024, Eos accounted for just over 1% of all STRs submitted.

232. FIs and VASPs are also aware of their obligations to report suspicion in a timely manner and reporting occurs within a couple of days, with immediate reporting for TF suspicion. Most entities use software to monitor suspicious activities, including AI, to better monitor typologies matching higher risk scenarios. However, the AT also noted that supervisory authorities have identified material weaknesses in some VASPs' implementation of STR reporting obligations, with significant gaps in monitoring and detection practices (which were later addressed by the VASP in question) indicating uneven compliance across the sector. STRs are broadly in line with main predicate offences, fraud and illegal betting and gambling are the most identified and reported suspicious activities (see IO.6).

233. FIs and VASPs are generally aware that multiple reporting on a single suspicion is possible and whenever there is doubt on the nature of the suspicion, entities confirmed that they report on both ML and TF. However, except for banks, most FIs report suspicious activities related to TF to a limited extent, which is in line with their more limited understanding of TF risks described above. While banks account for the majority of TF-related STRs in absolute terms, the overall volumes remain somewhat modest when viewed in light of the central role of the banking sector in Türkiye's TF risk context. The nexus with a terrorist organisation remains the main criterion for reporting entities to consider that a case could present a TF suspicion, which limits the scope of potential TF detection. For exchange offices, this finding is coupled with the information that entities met onsite indicated that EDD measures are more frequently identified

once transaction-value thresholds are reached. This reliance on value-based triggers may limit the detection of TF cases involving low-amounts transactions, especially in light of the sector exposure to TF.

Box 3.3. VASP TF suspicion case study

As part of its monitoring activities, a VASP was made aware that a terrorist organisation posted on social media the links to three wallet address to receive funds. The VASP identified its clients conducting transactions with those wallets and filled TF STRs. As a result, foreign nationals were identified and designated by Türkiye under its domestic TF TFS regime.

234. FIs and VASPs understand their obligations related to tipping off. To prevent potential tipping off, most entities conduct trainings to their staff, with specific in-person trainings for the personnel most involved in commercial relations with clients. Reporting entities considered that MASAK's trainings have effectively supported further awareness of this obligation.

Table 3.5. STRs for FIs and VASPs

Institutions	2020	2021	2022	2023	2024	2025	Total
Banks	182 828	205 793	314 700	432 499	349 988	235 358	1 721 166
VASPs	0	2 233	20 569	48 678	63 603	53 490	188 573
MVTs	46 840	284 544	74 513	102 776	110 949	101 897	721 519
EOs	2 660	4 500	6 188	9 108	5 726	4 315	32 497
Capital Market Sector	368	692	595	897	1 218	1 088	4 858
NBFIs	2 070	3 286	4 073	3 921	5 790	5 021	24 161
Insurance	361	404	496	529	747	674	3 211
Precious Metals Intermediary	0	0	0	0	1392	717	2 109
Total	**235 127**	**501 452**	**421 134**	**598 408**	**539 413**	**402 560**	**2 698094**

Table 3.6. TF STRs for FIs and VASPs

Institutions	2020	2021	2022	2023	2024	2025*	Total
Banks	1 460	2 067	1 374	2 535	1 950	1 311	10 697
EOs	0	1	9	6	44	27	87
VASPs	0	40	411	368	577	500	1 896
MVTS	158	403	937	938	930	1 381	4 747

Note: *as of November 2025.

3.4.4. Internal controls, procedures and audit to ensure compliance

235. FIs and VASPs generally demonstrate a strong understanding of their AML/CFT obligations and have established internal controls and procedures appropriate to their business activities. Entities, especially in the highest risk sectors, have a developed AML/CFT culture, reviewing their compliance policies annually or at least every 1–3 years and have formal procedures in place to support these policies, with coverage rates above 90% across most sectors. This is in line with supervisory findings, especially in the banking sector where infringement to AML/CFT requirements have steadily decreased over the reporting period.

236. While most FIs and VASPs have dedicated units to assess compliance risks, the presence of such units is significantly less consistent among EOs– which are in essence much smaller actors yet considered as medium-high risk. Türkiye's framework applies a risk-based approach that differentiates EOs by size and

business activities. Under this approach, the obligation to assign compliance officers and establish a compliance programme applies only to larger exchange offices (Group A), while smaller exchange offices (Group B) must appoint an exclusively designated compliance officer; however, they are not required to implement a compliance programme, despite the sector being assessed as medium-high risk. As there is no mandatory requirement for compliance programs for Group B EOs, the coverage and sophistication of compliance controls remain uneven, particularly among smaller entities. While the NRA identifies risk-reducing factors for Group B EOs relating to limitations in activities and lower business volumes, it also notes that the lack of a requirement to employ an internal control officer constitutes a risk-increasing factor. At the same time, although the authorities consider that Group B exchange offices are typically less exposed to ML/TF risks, weaknesses in internal control arrangements limit the effective and consistent implementation of AML/CFT controls within a sector assessed overall as medium-high risk.

237. Training and certification programs for compliance staff are widely implemented, except among exchange offices, and regular measurement and evaluation of training activities are reported by FIs and VASPS to a large extent.

238. Overall, FIs and VASPs have internal controls, procedures, and audit mechanisms in place especially for the highest risks sectors but to a lesser extent for EOs. . For EOs, these differences reflect the fact that Group B entities are not subject to the same legal requirements as Group A EOs. Internal audits under AML/CFT legislation are conducted at least annually by the vast majority of institutions while periodic independent audit services are also resorted to, though with more variation. Where applicable, group-level internal controls and audit requirements are implemented, despite some variation depending on the sector and group structure.

239. However, supervisors also reported that one of the common shortcomings for FIs and VASPs, is the minimal amount of resources allocated to the compliance units in comparison with other units and in light of the entities size and materiality. For more recent entities, especially VASPs, and smaller actors, MVTS and EOs, this may constitute a contributing background factor to the still elevated number of identified shortcomings with AML/CFT obligations, especially on CDD and to a lesser extent STR requirements (see 3.6).

3.4.5. Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

240. The Assessment Team did not identify any legal or regulatory requirements impeding implementation of AML/CFT obligations and mitigating measures in Türkiye.

3.5. Supervisors risk-based monitoring or supervising compliance by FIs and VASPs

241. Türkiye supervises FIs and VASPs following a RBA. High and medium risks entities are subject to frequent onsite inspections and all entities can be inspected offsite or as part of a specific thematic review with entities' risk scoring reassessed on a yearly basis. For VASPs, the supervisory framework was recently strengthened, and supervision is only effective to some extent. Although recent on-site inspections show a marked decrease in the proportion of VASPs found in violation, the supervisory framework cannot yet be considered fully effective. The sectoral supervisor has only recently changed, and at the same time the regulatory requirements for VASPs have been significantly tightened. The new licensing process is still ongoing, which means that all VASPs still continue to operate under transitional arrangements. As a result, the supervisory system is still in the process of stabilising, and its effectiveness cannot yet be assessed as fully achieved.

242. As a result of the findings of 2019 MER and ICRG Action Plan, Türkiye adopted a risk-based supervision (RBS) approach in 2020 to prioritise the supervision of highest risk sectors and highest risk entities within each sector. Dedicated protocols between MASAK and sectoral supervisors have been signed establishing principles and procedures for information exchange, co-operation and co-ordination in RBS of FIs and VASPs. MASAK, as the main AML/CFT supervisor, prepares annual supervision plans for all FIs and VASPs. The Threat & Vulnerability WGs and the sectoral risks analysis working groups (see 3.2) provide a platform for MASAK to exchange with sectoral supervisors as well as the private sector and the development of the sectoral risk assessments support the definition of yearly supervisory programs.

243. Türkiye's RBS methodology requires obliged entities categorised as high-risk to be supervised every year, and obliged entities categorised as medium-risk to be supervised every three years at the latest. The AML/CFT supervision programmes prioritise the on-site supervisions of higher risk sectors, as determined by Türkiye's national risk assessments banks, including VASPs, MVTS and EOs. In this context, it is noteworthy that, based on Türkiye's entity-level risk-scoring, approximately 5% of FIs and VASPs in sectors assessed as high or medium-high risk are classified as high risk at the entity level (see 3.2).

244. The supervision of compliance by FIs and VASPs is carried out through three types of supervisory activities. First, dedicated AML/CFT supervision programmes are defined annually by MASAK's Supervision of Obligations Department and are conducted either by MASAK's Treasury and Finance Experts, sectoral supervisors, or other staff listed below in Table 3.7 under the guidance of MASAK's Supervision of Obligations Department. Those onsite inspections aim at assessing the compliance status of the reporting entity against AML/CFT obligations. Second, prudential supervision conducted by sectoral supervisors. Even though those are not targeted at AML/CFT obligations, related shortcomings might be identified by the sectoral supervisor (e.g. CDD requirements, BO, etc.) and are referred to MASAK for further examination. Third, "case-based AML/CFT inspections", outside the scope of pre-planned activities, to determine whether any AML/CFT or prudential obligation has been violated. As mentioned above, the entity-level risk score is updated yearly, yet Türkiye cannot manually change – over the course of the year - the risk score to take into consideration new or emerging information that would impact the risk score of a specific entity. Nevertheless, this can be mitigated by ad hoc supervisory actions even in the absence of a revaluation of the entity risk score.

245. Those three types of monitoring activities are complementary and both onsite and off-site inspections are resorted to, allowing for a close monitoring of the financial sector. The scope of the case-based supervision can be as encompassing as the ones conducted within the scope of a programme, or it can be only on one obligation. Supervisory activities are applied in line with entities' risk profiles and are supported by close and ongoing engagement between MASAK, sectoral supervisors and obliged entities, including guidance and outreach activities. In practice, this approach has contributed to improved compliance, particularly at the level of individual institutions. For instance, in 2022 ten banks were supervised as case based only on their periodical reporting obligations. Parts of these supervisions can be conducted off-site, appointed supervisors can request information and documents (e.g. information on customers, transactions, products and services, policies, procedures, systems used etc.) from the reporting entities and evaluates them off-site. This information is then used to determine the areas of focus for the on-site supervision.

246. MASAK's Supervision of Obligations Department consists of 33 staff members fully dedicated to AML/CFT supervision. The Department prepares the annual AML/CFT supervision programmes. Beyond these dedicated resources, the Department also assigns the staff listed in Table 3.6 to conduct AML/CFT supervisory activities. These staff members can perform AML/CFT supervisory tasks alongside other responsibilities (e.g. prudential supervision in the case of sectoral supervisors) and are therefore not exclusively dedicated to AML/CFT supervision.

Table 3.7. Staff that can conduct AML/CFT supervision alongside their other responsibilities

Supervisors	Number of staff for supervision (as of June 2025)
MASAK (Treasury and Finance Experts)	129
BRSA	245
CMB	178
CBRT	47
ISPRA	50
Trade inspectors	293
Total	846
Others (Tax Inspectors + Treasury controllers)	6 816

247. The integrated approach between MASAK and sectoral supervisors ensures that prudential and AML/CFT supervision are complementary. After completing on-site examinations, the examiners submit their reports to MASAK. The Supervision of Obligations Department reviews these reports to ensure compliance with MASAK's reporting standards and to identify any legal or substantive errors. Reports recommending criminal penalties are forwarded to the relevant PPOs.

248. While the framework for co-operation is established, its practical implementation could be strengthened. Opportunities exist to deepen ML/TF risk understanding among sectoral supervisors (see 3.2) which have lesser expertise to carry out AML/CFT examinations in some technical areas, particularly when they require in-depth evaluation (e.g., transaction monitoring scenarios, sanction screening system rules, customer risk scoring models, etc). Addressing those challenges would further improve the effective supervision of FIs and VASPs.

249. In line with its ICRG Action Plan, MASAK's resources dedicated to Supervision of Obligations Department have been strengthened since the 2019 MER, from 12 staff members to 33 as of 2025. As of the time of the onsite visit, MASAK indicated that recruitment was ongoing, and further staff could be allocated to the supervision department. However, MASAK supervision department oversees compliance for FIs, VASPs and DNFBPs, it receives and analyses the reports of all sectoral supervisors, and is in charge of taking further actions, including issuing sanctions. Even though MASAK relies on sectoral supervisors, those do not have dedicated AML/CFT units nor specialised staff. In light of MASAK's broad prerogatives and pivotal role played by the Supervision of Obligations Department across all sectors, in conducting and co-ordinating AML/CFT supervision across all sectors, the resources of this department would benefit from further strengthening.

250. While Türkiye has a broad pool of examiners who may conduct AML/CFT inspections, the effectiveness of supervision may be affected by the distribution of AML/CFT expertise across supervisory authorities. MASAK's Supervision of Obligations Department, which consists of staff fully dedicated to AML/CFT supervision and with the highest level of AML/CFT expertise, plays a central role in risk-based planning and oversight. Alongside this, sectoral supervisors integrate AML/CFT supervision into their wider supervisory mandates (e.g. prudential supervision), reflecting Türkiye's holistic supervisory model. However, sectoral supervisors' do not have dedicated AML/CFT staff and expertise. This can impede the effective supervision of some sectors, especially high-risk sectors with emerging actors and complex ML/TF typologies. As mentioned above, CMB's understanding of VASP-related ML/TF risks is still developing. Supervising VASPs is a new responsibility for CMB and while staff have received general AML training, there are no AML/CFT specialists. This gap in risk comprehension could, to some extent, undermine the ability to prioritise resources and tailor supervisory actions to the sector's high-risk profile.

251. Since the legislation for licensing VASPs is relatively recent and VASPs have been obliged parties since 2021, the AML/CFT supervision of VASPs was initially conducted by experts from the Treasury

employed at MASAK. Since 2025, VASPs AML/CFT supervision has been conducted by CMB in addition to the supervision of capital market intermediaries and portfolio management companies.

252. The number of supervised obliged entities significantly increased over the reporting period and Türkiye prioritises the supervision of higher risk sectors. Supervision activities are conducted in line with entities risk profile to a large extent. All entities considered as high risks are subject to a yearly onsite inspection, across all sectors. In addition, while medium risk entities are required to be supervised at least every three years, those operating in the highest risk sectors are prioritised for selection in annual supervision programmes, ahead of medium risk entities in medium/low risk sectors. As a result, for banks, VASPs and EOs, all high and most medium risk entities are monitored each year, in line with a risk-based approach.

253. During onsite visits, supervisors mainly focus on the application of CDD requirement as well as the implementation by reporting entities of enhanced due diligence in higher risk scenarios and to also review the internal controls in place to mitigate risks. With regard to BO, the supervisory guidance documents direct supervisors to assess whether reporting entities identify the natural persons or legal persons holding more than 25% of the shares in a legal entity when establishing a permanent business relationship with legal persons registered in the trade registry. However, the guidance documents do not instruct supervisors to consider whether reporting entities have taken into account other forms of control in the identification of the BO, such as control exercised through means other than ownership. As a result, the supervision may overlook at such situations.

254. For banks, during onsite audits the institutional risk assessment is constantly reviewed, yet authorities did not provide statistics on infringements with those obligations. Customers risk scoring and mitigating measures process are also reviewed, including whether those have been included in internal policy documents and if the staff are aware of those. Supervisors assess internal controls including in conducting interviews with employees to assess awareness levels as well as the adequacy of compliance units staffing in comparison with other departments of the reporting entity. High risk transactions and customers are also systematically monitored in the course of inspections, using automated tools. The scope of the onsite can be further defined with an offsite preliminary assessment based on internal documents from the reporting entity (internal policies, risk scenarios, etc.). Supervision programs for banks can take from several weeks to a year depending on the size and complexity of the case.

255. For VASPs, similar scrutiny is applied to CDD measures and internal controls, especially KYC measures taken when the onboarding of a new client is done remotely. As VASPs is a newly regulated sector, the presence of a compliance unit is also systematically checked as well as the presence of internal policies and procedures. Türkiye also set up a repository for all VASPs customers who are allocated a unique number. Supervisors monitor if VASP have referred their customer in the repository and if the transactions related to the client have been reporting accordingly. Supervisors are also resorting to electronical tools to monitor transaction and potential absence of STR reporting. As per the recent supervision and ongoing licensing process of VASPs in Türkiye, the monitoring of AML/CFT compliance for VASPs is to be further developed.

256. For MVTS and EOs, the focus is on the type and level of transactions carried out as well as the implementation of CDD measures which generally represents a challenge in the sector. Transactions among MVTS or between MVTS/exchange offices and other high-risk sectors, such as DPMS, are also given additional scrutiny by supervisors. For exchange offices, supervisors also screen video footage to detect any potential suspicious activity.

257. For NBFIs and Insurance, representing the lowest risk level for FIs, supervision is conducted yearly for high-risk entities and to a lesser extent to medium risk entities. The monitoring is conducted on the overall compliance with AML/CFT obligations.

258. Table 3.8 provides an overview of AML/CFT supervisory activities by year. For each year, the table sets out the number of obliged entities included in the annual supervision programme (Prog), the number of case-based (ad hoc) supervisions conducted outside the programme (Case), and the number of entities classified as high- or medium-risk based on risk analyses. The final columns present cumulative figures for the period covered. For example, in 2024, 31 banks were classified as high- or medium-risk, of which 15 were inspected as part of the annual supervision programme and one through a case-based supervision.

Table 3.8. Risk-based supervisory activities

Sector	2020			2021			2022			2023		
	Prog	**Case**	**Total High Medium entities**	**Prog**	**Case**	**High Medium**	**Prog**	**Case**	**High Medium**	**Prog**	**Case**	**High Medium**
Banks	15	5	25	16	0	18	21	10	21	15	0	28
VASPs	0	0		0	5		13	0	19	22	1	24
MVTS	17	1	27	14	1	26	20	1	27	20	6	33
EO	35	1	125	36	3	118	63	3	272	72	2	156
CM	21	0		24	0		29	0		12	0	
NBFIs	14	0	26	17	0	27	24	0	33	16	1	49
Insurance	8	0	17	9	0	19	14	0	26	0	0	not av
PMIs	0	0	not av	0	4	not av	4	0	11	0	0	not av

Sector	2024			2025			Total		
	Prog	Case	High Medium	Prog	Case	High Medium	Prog	Case	High Medium
Banks	15	1	31	22	0	39	**113**	**16**	**123**
VASPs	23	0	38	27	0	43	**96**	**6**	**81**
MVTS	33	1	40	33	0	45	**144**	**10**	**153**
EO	80	0	164	117	0	323	**450**	**9**	**835**
CM	19	0		17	0	29	**105**	**0**	**0**
NBFIs	14	0	42	19	0	41	**127**	**1**	**177**

Insurance	2	0	2	10	0	19	**35**	**0**	**64**
PMIs	2	0	2	3	0	3	**8**	**4**	**13**

259. Not all entities in high-risk sectors have been subject to supervision over the reporting period. A total of 50 banks (out of 63) have been subject to AML/CFT supervisions since 2021, either through supervision programme, case-based monitoring or both. Authorities indicate that out of the remaining ones, 9 are either recently established with limited banking activities or investment and development banks not accepting deposits and participation, only providing credit for investments and hence being consider much lower risk. Since 2020, only a small number of payment and e-money institutions (10) have not yet been subject to AML/CFT supervision, most of which obtained their licences only recently, whereas a much larger number of exchange offices (526) remain unsupervised over the same period, demonstrating a more limited supervisory coverage in that medium-high risk sector. With regard to NBFIs, out of the 48 Factoring, 20 Leasing and 24 Financing companies (92 in total), 30 of those have not been supervised since 2021. Of those, 7 of them were established after 2022 and have limited activity. However, NBFIs are not considered high nor medium-high risks.

3.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate and dissuasive sanctions on FI and VASP compliance

260. Supervisory authorities employ remedial actions to a large extent where breaches in compliance with CDD and STR obligations are detected. The adoption of the RBS approach in 2020 has led to a significant increase in the number of compliance supervisions - particularly on high-risk entities.

261. Over the reporting period and in line with Türkiye's ICRG Action Plan there has been overall significant improvements in the AML/CFT compliance and the overall compliance culture of the FIs and VASPs due to enhanced supervisory actions, although significant weaknesses continue to be identified in certain sectors, notably EOs. Onsite examinations find less issues for FIs and VASPs with past enforcement records. The representatives of FIs and VASPs met during the onsite praise the quality of the relationship with their supervisors and provided tangible examples that supervisory activities had positive impact in supporting their compliance with AML/CFT requirements.

262. Supervisory authorities impose sanctions in relation to their scope of competence as defined by law. MASAK is the sole authority entitled to issues sanctions with regard AML/CFT breaches while sectoral supervisors apply sanctions on their respective field of competence. As described above, there is close co-ordination among supervisory authorities, if a sectoral supervisor detects a potential ML/TF infringement in the course of its monitoring of a reporting entity, the case is referred to MASAK for further actions.

263. MASAK can impose several types of formal remedial supervisory actions depending on several factors, including whether the breaches constitute criminality; their severity, the constancy and repetitiveness of violations; the compliance history of the FI or VASP.

264. Türkiye's approach is firstly directed at enhancing compliance by issuing written warnings, especially to entities in violation for failure to develop training, internal supervision and risk management system or assign a compliance officer. When shortcomings are identified over the course of monitoring activity, those are listed and sent to the reporting entity.

265. However, concerns arise as to whether sanctions related to internal controls are sufficiently severe and dissuasive. The very limited use of such fines suggest that the current practice may not deliver

outcomes that are proportionate to risks or sufficiently dissuasive across the FI and VASP sectors. For certain breaches, namely internal audit, trainings and risk management system, a remedial time of not less than 30 days, is given to the entity to address the shortcomings and an administrative fine is imposed only if deficiencies persist after the remedial period. The legislation does not prescribe a maximum period for obliged entities to remedy identified shortcomings. The timeframe is determined on a case-by-case basis according to the nature of the deficiency and communicated to the obliged entity; in practice, the period generally does not exceed 60 days. In most instances a written warning has been sufficient for the obliged party to take necessary actions. Out of 77 reporting entities, only two failed to address their deficiencies within the given time. The imposition of administrative fines on the obliged entity and the senior manager, along with the second written warning, ensured that these two obliged parties also addressed their deficiencies. While deficiencies in internal controls may in some cases coincide with, or give rise to, additional CDD or STR breaches that are sanctioned accordingly, the fact that even systematic and severe AML breaches can be resolved through a written warning—provided deficiencies are corrected within the grace period—indicates that the regime in practice allows FI and VASP entities to avoid proportionate and dissuasive sanctions as long as remedial action is taken within the allotted timeframe. In this respect, the current sanctioning regime is not fully proportionate to the risks and is not sufficiently deterrent to prevent non-compliant behaviour especially in cases of severe breaches.

266. Türkiye applies a risk-based methodology to determine annual supervisory programmes, taking into account the results of previous AML/CFT inspections. FIs and VASPs with repeated or serious violations, as well as those not previously supervised, receive higher risk scores and are more likely to be included in subsequent supervisory cycles. Entities that are subject to repeated supervision generally display significantly fewer or no violations in follow-up inspections, indicating that supervisory engagement leads to improved compliance for the individual institution concerned over time.

267. When criminal offences are detected, MASAK files a criminal complaint to the public prosecutor and can in parallel suspend the reporting entity. Over the reporting period, MASAK has filled 11 criminal complaints against FIs for record keeping infringement. Judicial penal procedures can also apply in other cases of serious breaches, such as breaches of STR confidentiality and not providing information and documents when requested. These offences did not occur during the reporting period, so in general judicial proceedings comparatively lower than administrative fines. In 2024, there were 11 referrals to the public prosecutor's office for such breaches, indicating that while criminal enforcement measures exist and can include custodial sentences, their application is limited in practice.

268. Supervisors have a wide range of administrative sanctions available. For CDD and STR breaches, administrative fines are imposed on a per-breach basis through fixed statutory amounts, with a mandatory transaction-based minimum threshold applying to FIs, as set out in the AML Law. In line with Türkiye's ICRG Action plan, the amount of administrative fines has significantly increased since 2020. In addition, the amount is reviewed on a yearly basis according to the revaluation rate in order not to lose value due to inflation and in accordance with the Tax Procedure Law. Accordingly, the amount of the applicable administrative fines for CDD, STR and periodic reporting breaches has significantly increased since 2020, ensuring that available sanctions remain dissuasive. Authorities can also suspend or revoke reporting entities depending on the persistence or severity of the violations.

Table 3.9. Applicable administrative fines for FIs and VASPs (applicable per breach of obligation)

Obligation	Applicable Administrative Fine Amounts (EUR, per breach)					
	2020	2021	2022	2023	2024	2025
CDD	1 200	1 309	1 783	3 975	6 299	9 067
STR	1 000	2 182	2 972	6 626	10 499	15 111

Periodic Reporting	1 200	1 309	1 783	3 975	6 299	9 067
Max Amounts (Annual)	800 000	872 880	1 188 863	2 650 331	4 199 715	6 044 650

269. Sanctions are largely tied to the number of concrete violations identified in relation to customer-specific CDD and STR obligations. In contrast, even extensive systemic weaknesses, such as inadequate governance, training, monitoring, procedures or identifying and reporting suspicious transactions, technical capacity, and risk assessment, are systematically addressed through a two-stage supervisory response, whereby a written warning accompanied by a remedial period, constitutes the initial enforcement action and remains the sole measure where the deficiencies are remedied within the prescribed timeframe. This imbalance, where isolated customer-level breaches attract stronger sanctions than broad structural failings, weakens the overall proportionality, effectiveness, and deterrent impact of the supervisory sanctioning framework. This raises concerns primarily in relation to the supervisory responses to serious or systemic shortcomings in governance, internal controls and risk assessment frameworks, rather than to the availability of sanctions for individual CDD or STR breaches.

Box 3.4. Deficiencies in AML/CFT internal framework control

During an on-site inspection, supervisors identified deficiencies in the bank's risk-based transaction monitoring and internal control framework, which limited the effective detection and escalation of suspicious activity. In particular, transactions were not systematically verified against supporting documentation to assess their consistency with customers' financial profiles, customer information and documentation were not kept up to date, and communication and co-ordination between internal departments were inadequate. As a result, the compliance unit was not adequately or sufficiently informed, and monitoring and control activities were not carried out effectively.

A written warning was issued to the bank, requiring it to address the identified deficiencies and to implement specified corrective and remedial measures within 60 days. After the given time, the bank reported that it had reviewed the relevant internal regulations and implementation processes, taken corrective and remedial measures to address the identified deficiencies, and implemented these measures supported by substantiating information and documentation. In this context, it was assessed that the bank had effectively established and implemented the risk-based control and monitoring systems envisaged under Article 5 of the AML Law. No administrative sanctions were imposed. However, the bank was included in the following year's supervision programme to monitor the continuity and effectiveness of the measures taken.

270. Also, enforcement actions for PEP-related obligations are not sufficiently risk-based or proportionate. Emphasis is placed on the presence of individual PEP customers and on whether EDD has been applied to them, rather than treating weaknesses in preventive controls as breaches warranting stronger measures. Since PEP obligations were introduced in 2022, only one entity (a bank) has been sanctioned for deficiencies in EDD for PEPs, questioning the effectiveness of monitoring against PEP requirements. Türkiye's NRA identifies payment institutions as a medium-high-risk sector, partly due to corruption vulnerabilities; however, even in a case where a payment institution lacked any policies or procedures for applying EDD to PEPs, only a written warning was issued because no PEP customers were identified in the customer base and the institution's non-compliance could not be demonstrated in relation to a specific customer. This approach, which is not commensurate with the systemic nature of the deficiency or with the sector's risk profile, undermines the dissuasive effect of enforcement and limits the overall effectiveness of supervision.

Box 3.5.Case 1 (PEPs)

Supervision identified that PEPs were neither classified as a high-risk customer group in the payment institution's compliance programme nor in its internal policy documents, and that EDD measures applicable to PEPs were not set out in these documents. This indicated policy-level weaknesses in the application of the risk-based approach. However, during supervision, the authorities conducted testing of the institution's automated screening tool, which successfully identified a mayor of a city in Türkiye as a PEP. Screening of the institution's customer base also revealed that it had no PEP customers. As no breaches relating to PEP-related EDD occurred in practice, no administrative fine was imposed. Instead, a warning letter was issued and a period of time was provided for the institution to remedy the identified deficiencies in its policies and procedures.

Table 3.10. Fines issued for CDD and STR breaches (2020 – 2025)

Sector	Number of supervised obliged entities	CDD		STR		Total Admin Fines (EUR)
		Obliged entities in violation	Administrative Fine (EUR)	Obliged entities in violation	Administrative Fine (EUR)	
Banks	98	13	478 000	13	1 648 400	2 126 400
VASPs	64	27	756 800	23	1 393 400	2 150 200
MVTS	114	45	7 633 300	20	10 305 700	17 939 000
EO	295	178	4 491 500	25	207 200	4 698 700
Capital Market	105	14	272 800	6	18 100	290 900
NBFIs	86	19	186 700	10	18 000	204 700
Insurance	33	4	31 400	0	-	31 400
PMIs	10	4	32 600	2	82 900	115 500

Table 3.11. Application of sanctions for deficiencies in AML/CFT internal control, risk management and compliance arrangements

Obligation	Application
Article 5 (1) of AML Law no. 5549 Developing training, internal supervision and control and risk management systems, assigning compliance officers in FIs.	**2021** 13 obliged entities who were in violation of this Article were sent a written warning and a period of time (not less than 30 days) was given. All obliged entities addressed the deficiencies within the given time. **2022** 21 obliged entities who were in violation of this Article were sent a written warning and a period of time (not less than 30 days) was given. All obliged entities addressed the deficiencies within the given time. **2023** 9 obliged entities who were in violation of this Article were sent a written warning and a period of time (not less than 30 days) was given. 7 of these obliged entities addressed the deficiencies within the given time. 2 of these obliged entities failed to address the deficiencies and 1.518.153 TRY administrative fine (each) was imposed. After that, a second written warning and period of time was given. Both of these obliged entities addressed the deficiencies within the given time. **2024** 34 obliged entities who were in violation of this Article were sent a written warning and a period of time (not less than 30 days) was given. Actions taken by the obliged entities are being evaluated to determine whether the deficiencies were addressed or further action is necessary.

271. For the banking sector, 98 on-site supervisions (both within the scope of a programme and cased based) were carried out over the reporting period. On the basis of these on-site findings, few banks were found to be in violation of their CDD/STR obligations and those that were had very few violations. This is reflected in the low amounts of imposed administrative fines. Between 2021 and 2024, only five banks were subject to a written warning and a remedial period in response to deficiencies in AML/CFT internal control, risk management and compliance arrangements The assessment team reviewed, for instance, a case example in which supervisors, during an on-site inspection, identified insufficient algorithmic analysis infrastructure to detect transaction repetitions and systematic movements and transactions were not subjected to specific limits based on their risks.

272. As part of its offsite review of the annual survey sent to banks, MASAK also identified that some entities were carrying out derisking with considered high risk customers, such as NPOs or VASPs, which was confirmed during the onsite. This finding supported further outreach to the sector to sensitise against such practices, yet NPOs and VASPs met during the onsite confirmed that their access to the financial system via banks was not hindered. In addition, a 2023 survey by the Banks Association of Türkiye shows that banks apply markedly restrictive onboarding practices toward certain customer groups. VASPs faced by far the highest refusal levels (approximately 40 %), followed by payment and electronic money institutions (approximately 25%), with EOs also encountering notable rejection rates (approximately 17%). Authorities further explained that some banks only prefer to work with PEMIs within the same financial group, which contributes to higher rejection rates. They also noted that rejection rates for VASPs are expected to decrease following the introduction of the new licensing regime; however, at the time of the onsite, there was no evidence of such an impact, as no licences under the new regime had yet been granted.

273. VASPs have been obliged entities since 2021, and initial supervision showed that all entities subject to inspections had numerous violations of their AML/CFT obligations. As a result, Türkiye's enhanced supervisory activities by including more VASPs as part of the supervision programmes (from 5 VASPs in 2021 to 23 in 2023 and 2024). İn addition, MASAK enhanced outreach activities, issuing specific guidance for VASPs and conducting further trainings. Authorities reported that recent shortcomings were linked to the absence of technology supported process to adopt enhanced measures for high-risk customers and

transactions. Overall, the sector has been issued for more than EUR 2 million fines. Ongoing licensing process for VASPs is expected to reduce the number of actors in the sector and support further compliance, yet this process was still ongoing at the time of the onsite.

274. MVTS have been the most heavily fined sector over the reporting period with EUR 18 M fines allocated. The ratio of MVTS with violations in comparison with the overall the number of supervised entities has steadily decreased over the reporting period, demonstrating in overall progress in sectoral compliance with AML/CFT obligations and effectiveness of the supervisory activities and remedial actions taken. While 90% of the MVTS supervised were in violation with their CDD obligations in 2020, this ratio dropped to 15% in 2024. While improvements have been achieved, some singular significant cases were also identified, where MVTS are used for illegal betting, ML or TF, emphasising the need for close monitoring of the sector and potential enhanced remedial actions.

275. Exchange offices are the second highest fined sector for breaches in CDD/STR obligations and the one presenting the highest number of breaches. Despite taking into consideration the high number of entities in the sector (over 750 exchange offices), the fact that in 2024 65% of the 80 supervised entities were in violations of their CDD obligations is concerning. The number of Eos found in breach has increased steadily over the period, while the total amount of administrative sanctions has grown more moderately and not in direct proportion, despite the fact that applicable administrative fines are increased every year. Authorities consider that the low level of administrative fines imposed in light of the number of violations illustrates that the entities' violations were not major nor numerous. At the same time, it is noted that the sanctions imposed can, in certain cases, reach levels that are significant and proportionate relative to the capital and financial capacity of the obliged entities concerned. Authorities also explained that, although measurable improvements are observed at the level of individual EOs once they have been subject to supervision, these entity-level gains are not reflected in the aggregated annual statistics. According to the authorities, this is primarily due to the structural composition of the sector: each annual supervision cycle incorporates a significant number of entities that are being examined for the first time and that, according to the authorities, systematically exhibit a higher likelihood of non-compliance. The authorities further noted that this phenomenon is particularly pronounced in the exchange office sector, which comprises a very large number of supervised entities and a high turnover in the pool of entities selected for supervision.

276. In addition, the EO sector accounts for the highest proportion of enforcement cases among FIs and VASPs involving deficiencies with respect to risk management, internal governance and other AML/CFT requirements under AML Law Act. 5, representing more than 61% of such cases. These cases follow a graduated enforcement process, whereby a written warning and a remedial period to address the identified deficiencies are issued as a first step, and an administrative sanction may be imposed only where deficiencies are not remedied within the prescribed timeframe.

277. Consequently, the continued identification of a high number of breaches in the EO sector could be seen as an indication of the broad compliance weaknesses across the sector as a whole. Even after some entities have undergone inspection, received corrective instructions and, in many cases, demonstrated improvements upon re-inspection, the overall statistical profile remains dominated by newly identified violations. From a supervisory effectiveness perspective, this pattern raises concerns regarding the capacity of the current sanctioning framework to generate a sufficiently robust dissuasive effect at the sector level. While sanctions may induce compliance improvements within the entities directly subjected to them, the consistently high incidence of violations—especially among first-time supervised entities—suggests that the signalling effect of sanctions is not strong enough to incentivise preventive compliance across the wider sector.

278. Despite the capital market, NBFIs, Insurance and precious metal intermediaries having been subject to less supervisory activities in line with the risk-based approach, MASAK identified violations for CDD and

STR violations and allocated administrative penalties. Overall, the supervised entities demonstrated good level of compliance.

279. MASAK does not publish its enforcement actions, including sanctions and remedial measures, not even in an anonymous form, limiting transparency and undermining the potential deterrent effect of its sanctioning regime. While MASAK communicates annually through its activity report, the information made public is limited only to high-level aggregated data, such as the total number of sanctions imposed and the number of obliged entities sanctioned each year, together with a general reference to the legal basis for imposing sanctions. The activity report does not provide a breakdown of sanctions by sector, nor does it distinguish sanctions by type of breach, or severity, and it does not include case examples, even in anonymised form. No information is published on remedial measures. However, during the course of its outreach activities to each sector, MASAK communicates on the main regulatory breaches. Nevertheless, some FIs considered that publishing enforcement actions could have a positive impact for sectoral compliance, while others consider that it would be too prejudicial to the sanctioned entities. The current lack publication of enforcement actions, including sanctions and remedial measures, imposed within each sector diminishes the dissuasive impact of the sanctioning framework and hinders the possibility of those specific examples of non-compliance contributing to strengthened compliance in other entities than the one directly affected by the decision. Publication of enforcement actions would provide the financial sector with the clarity and visibility to support enhanced compliance.

Box 3.6. Sanctions for AML/CFT breaches – case studies

The case below illustrates that prudential supervisors can also impose sanctions in situations where the identified deficiencies cut across both sector-specific regulatory requirements and AML/CFT legislation.

Case 1: It was identified that B Investment Securities A.Ş., when entering into electronic contracts with clients for opening investment accounts, implemented practices that were contrary to the legislation in relation to identification and customer due diligence obligations. According to the findings, the institution was carrying out remote identification procedures through an external service provider, E Information Technologies A.Ş., but was opening accounts without completing the video call step. It was found that out of 12,288 clients, only 230 had completed the video call, and the remaining clients had accounts opened without video verification. It was also identified that in some video calls, image and sound quality were inadequate, the serial number of the client's ID card was not read out loud, and that the video call was conducted after the account opening. The non-compliant implementation of remote identification procedures by B Investment Securities A.Ş. has constituted a breach both of capital markets legislation and MASAK regulations. This has led to unfair competition among investment firms, undermined investor confidence and been deemed contrary to the essence of customer due diligence obligations. Taking into account the severity and persistence (in file of several clients) of the breach and the high number of clients, authorities departed from the minimum fine level and imposed administrative sanctions for a total of approx. EUR 260 000.

The case below illustrates how findings originating from MASAK's analytical work can be operationalised through sectoral supervision, including in situations where sanctions are imposed under sector-specific legislation rather than the AML Law.

Case 2: The findings of an analysis report prepared by MASAK and submitted to BRSA, were examined by the BRSA on-site inspection team, resulting in the following findings at P Bank:

- It was assessed that the change made to the criteria of the program used by the bank in customer identification processes weakened the effectiveness of the customer identification process.

- It was noted that customers could open multiple accounts and obtain IBANs to conduct transactions below the limits, thereby falling outside the monitoring scenarios.
- It was noted that the failure to share the information and documents required by the Compliance Department during its audits with TKB constituted a violation of the Internal Systems Regulation.
- It was noted that despite the customer volume doubling in approximately 5 years as a result of high growth appetite, the number of personnel in internal systems units remained relatively low, and that an appropriate number of qualified personnel should be assigned.
- It was noted that the program used in the customer identification process was not fit for purpose, and that the tools used by internal systems units needed to be updated to meet current conditions.

An administrative fine amounting to approx. EUR 152 000 was imposed on the Bank, and instructions were given to remedy the deficiencies. The sanction was imposed by BRSA under sectoral legislation (Banking Law), and not pursuant to the AML Law. Currently, the audit team assigned to this Bank is evaluating whether actions have been taken.

The case below illustrates the use of supervisory measures to address breaches relating to internal control and internal audit arrangements

Case 3: During a supervision conducted at an MVTS, when internal audit activities were evaluated, it was determined that internal control was carried out by an expert, that the same person also carried out internal audit activities, and that this person worked under the management board member responsible for internal systems. It was also noted that no person was specifically appointed for internal auditing, no internal audit reports were produced, and therefore internal auditing and internal control activities were combined within the same person, which is forbidden by legislation. A written warning was sent to the reporting entity and a period of time was given for obliged party to address the deficiency.

The case below illustrates how the use of MASAK's Analysis and Evaluation Reports, together with supervision results from sectoral supervisors, in the preparation of supervisory programmes has proven to be beneficial. It also demonstrates that effective results can be achieved through close, co-operation between MASAK and the relevant sectoral supervisors.

Case 4: Analysis and Evaluation Report was prepared by MASAK to examine whether an MVTS was abused for illegal betting activities. This report was sent to CBRT as well. Additionally, this obliged entity was also included in the 2024 supervision programme. The supervision found that the MVTS did have control and risk management mechanisms but purposefully allowed opening of accounts to be used as fronts for illegal betting and ML, system alerts were ignored and not turned into STRs. Therefore, it was concluded that the MVTS was not simply abused for illegal betting and ML but also became a front for these activities. An administrative fine of over EUR 11,5 million was imposed for serious CDD and STR violations resulting from purposefully allowed conduct. CBRT, after carrying out its own audits, concluded that the MVTS's continued operation poses a threat to the security of payment systems and temporarily suspended the MVTS license and Savings Deposit Insurance Fund (TMSF) was appointed as trustee to the institution as well as the other members of the financial group, in which the payment institutions was the main financial institution.

4 Non-financial sector supervision and preventive measures

The relevant Immediate Outcomes considered and assessed in this chapter is IO.4.[26] The Recommendations relevant for the assessment of effectiveness under this chapter are R.22, 23, 28, 34 and 35 and elements of R.1, 29 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Türkiye has a licensing framework in place for all DNFBPs and conducts fit and proper checks to a certain extent. Responsibility is shared among several authorities and SRBs. The process is robust for accountants, lawyers and notaries. While authorities also perform fit and proper requirements for DPMS and REAs, those do not extend to associates of criminals. Türkiye detects unlicensed activities, in relation to DNFBPs, to some extent. However, the persistence of a high number of unlicensed actors in the REA and DPMS sectors reflects a lack of dissuasiveness of the sanctions allocated in those cases.

b) Türkiye has identified ML/TF risks across DNFBP sectors through a comprehensive risk assessment. MASAK demonstrates a comprehensive understanding of risks while sectoral supervisors' risk understanding is more limited and focuses more on risk mitigation measures than on actual ML/TF risks. Given MASAK's role as the primary AML/CFT supervisor, this difference in understanding is expected; however, enhancing sectoral supervisors' knowledge of ML/TF risks would improve their ability to carry out AML-related supervisory tasks effectively. Despite some positive steps taken by competent authorities, DNFBPs' understanding of ML/TF risks remains limited. In the DPMS and REAs sectors, the understanding of ML risks is more developed, especially for larger entities, while TF risk understanding is limited to awareness of TF related TFS obligations. Accountants, lawyers and notaries have a more limited understanding of ML/TF risks.

[26] When assessing effectiveness under Immediate Outcomes 4, assessors should take into consideration the risk, context and materiality of the country being assessed. Assessors should clearly explain these factors in Chapter One of the mutual evaluation report under the heading of DNFBPs, as required in the instructions under that heading in the Methodology.

c) Larger DNFBPs, particularly those that are part of international groups, generally understand their AML/CFT obligations and implement measures to comply with them, including using automated systems to verify BO information and monitor suspicious activity. DNFBPs have an overall understanding of the concept of PEP but identification is achieved to a limited extent. Except for DPMS, other DNFBP sectors barely report suspicious transactions, this is not in line with the risks they are exposed to especially for REAs, accountant and to a lesser extent lawyers. While larger DNFBPs apply internal controls as a group policy, there is a lack of such measures in smaller DNFBPs across all sectors.

d) Türkiye follows an RBA for the supervision of DNFBPs, all high-risk entities in the highest risk sectors (DPMS, REAs and accountants) are supervised yearly and medium risk ones have been supervised at least once over a three-year period. Nevertheless, supervision of the other sectors (lawyers and notaries is scarce and not in line with the risks posed by some entities in those sectors. The effectiveness of supervisory measures is impacted by supervisors' limited resources with AML/CFT expertise, leading to a marginal number of supervisory activities conducted over the reporting period in comparison with the overall size of the sector.

e) Supervisors have undertaken remedial actions and penalties mainly for non-compliance with CDD requirements. Over the reporting period, MASAK has undertaken significant efforts to increase DNFBPs' understanding of their AML/CFT obligations with the issuance of dedicated guidance and the conduct of numerous trainings for all sectors. Beyond the scope of CDD requirements, supervision is limited on other AML/CFT obligations and did not demonstrate a tangible impact on the sector overall compliance.

Key Recommended Actions (KRAs)

g) Strengthen DNFBPs' understanding of ML/TF risks and of their related AML/CFT obligations.

h) Increase supervisory capacities for DNFBPs, this could be achieved either through strengthening MASAK's resources allocated to supervision and/or enhancing AML/CFT expertise and dedicated staff for sectoral supervisors.

i) Develop a comprehensive understanding of the ML/TF risks lawyers are exposed to and ensure that high risk entities in legal (lawyers and notaries) and accounting sectors are monitored regularly.

Other Recommended Actions

a) Extend fit and proper requirements to associates of criminals to prevent them from being professionally accredited or holding or being the beneficial owner of a significant or controlling interest in a DNFBP.

Overall Conclusions on IO.4

Türkiye has a licensing framework in place for all DNFBPs, with fit and proper requirements being applied to prevent criminals, but not their associates, to enter the market. There is a significant number of actors performing activities without a license, which is being detected by competent authorities to some extent. However, the persistence of such activities in DPMS and REA sectors questions the effectiveness of sanctions imposed.

Türkiye has an overall good understanding of the ML/TF risks the DNFBP sector is exposed to, both at sectoral and entities' level. MASAK's robust understanding is the cornerstone for the definition of yearly risk-based supervisory programs leading to all highest risk entities in the higher risk sectors (DPMS, REAs, accountants) being supervised yearly while medium risk entities are supervised frequently. However, there is scarce supervisory focus on lawyers and notaries, despite those sectors performing some activities presenting important ML/TF risks. DNFBPs' supervision mainly focuses on monitoring CDD requirements while other AML/CFT obligations including suspicious reporting, for which DNFBPs generally do not demonstrate sufficient understanding, are barely monitored. Due to resource constraints, supervisory activities are also limited in light of the size of the sector.

DNFBPs' understanding of ML/TF risks is uneven. While larger firms with the highest risk sectors (DPMS and REAs) understand ML risks their sector is exposed to, there is limited comprehension by smaller entities and in the other sectors (accountants, lawyers and notaries). Outside the scope of TF related TFS, TF risks are not captured. This limited risk understanding is somehow mitigated by general awareness of AML/CFT obligations across all sectors. Yet, STR reporting, except for DPMs, remains negligeable and the lack of internal controls does not support further preventive measures. Supervisory actions undertaken, including remedial actions and sanctions, have contributed to raise awareness of AML/CFT obligations, but did not significantly improve overall compliance.

Türkiye is rated as having a Moderate level of effectiveness for IO.4.

Immediate Outcome 4

280. In Türkiye, all DNFBPs are subject to AML/CFT obligations. MASAK is the AML/CFT supervisor, meaning that it oversees compliance with ML/TF obligations for all reporting entities. There are several licensing and registration bodies as well as supervisory authorities for DNFBPs (detailed below). Casinos are forbidden by law in Türkiye.

281. For the assessment of the implementation of preventative measures and supervision for DNFBPs, the AT considered DPMS and REAs as the most important sectors in Türkiye and weighted these sectors the heaviest, in line with the medium-high risk ML/TF risk identified for those sectors in Türkiye's NRA. Accountants and lawyers were also weighted more heavily than the remaining DNFBPs given their important roles with domestic and foreign legal persons. Notaries were given lower importance.

4.1. Licensing, registration and controls for DNFBPs preventing criminals and associates from entering the market

4.1.1. Market entry controls

282. Türkiye has a licensing framework in place for all DNFBPs and conducts fit and proper checks to a certain extent, responsibility is shared among several authorities and SRBs.

DPMS and REAs

283. DPMS and REAs are licensed by the MoT. Applicants shall submit their application through the electronic system of the Ministry and the application is reviewed electronically, there is no face-to-face meeting with applicants. After the applicant submits the application through the systems, the relevant Provincial Directorate of Trade in the province where it carries out its activities reviews the documents uploaded by the applicant, as well as the data obtained from other integrated information systems. Some requirements are applied to DPMS and REAs applicants such as not being convicted of a crime, providing a tax registration number, registering with the relevant professional union, possessing relevant qualification. The fulfilment of these conditions is examined with supporting documents prior to the issuance of certificate of authorisation, within ten days from the date of submission.

284. In Türkiye, it is not compulsory to obtain the services of a REA to buy/sell a property.

285. BO information is indirectly checked. Applicants, either natural or legal person, have to provide their tax registry information and as taxpayers they need to file their BO information to Turkish Revenue Authority (TRA) as part of tax returns. Obliged entities can verify and identify discrepancies between the information provided to them during CDD process and through QR code provided by the TRA. If the applicant is a foreign legal person without a tax code, it would need to register to the TRA and disclose its BO information. The MoT does not have direct access to the BO information and does not consistently check the coherence between the information submitted by the applicant and the BO information as collected by the TA, but it can file a request to the TRA in case of suspicion.

286. However, under Türkiye's legal framework the fit and proper requirements do not extend to associates of criminals from being professionally accredited or holding (or being the beneficial owner of) a significant or controlling interest in a DNFBP (see R.28).

287. Authorities have rejected a significant number of applications. The most common reasons for the rejection of certificates in both sectors are similar, they include the submission of incomplete or incorrect documents to the system, errors in the document demonstrating the absence of tax debt to the tax office and the lack or absence of professional experience and professional training among the fields of activity listed in the applicant's professional union registration. The number of applications rejected is very high as any application missing one of the requested documents is automatically rejected and applicants must fill a new application.

Accountants

288. In Türkiye, accountants are either certified public accountant (CPA) or sworn-in public accountants (SPA), their licenses are issued exclusively by the SRB called TURMOB, and the licensing process is standardised. Specific requirements to enter the profession apply, following completion of the accountant exam, at least 4 years are required to obtain a CPA license. Whether the person meets the required conditions is examined prior to licensing, along with supporting documents. To become a SPA, one must work as a CPA for at least 10 years and then pass the competency exams. The most common reason for license applications being rejected is that the individual's criminal record does not comply with the law.

Lawyers

289. The Bar (SRB) is the licensing authority for lawyers. Lawyers need to have certain qualifications and the Bar reviews the applicant's file to ensure that none of the disqualifying conditions (such as criminal conviction, disciplinary issues, or ethical incompatibility) apply. Upon successful completion of an internship, the candidate must apply for inclusion on the bar register as a full attorney. The bar's executive board examines the application and makes a decision to approve or reject admission. Records of those whose admission requests are rejected are kept by Bar Associations and Union of the Turkish Bar Association. Lawyers whether they are corporate taxpayers or established as individual businesses are required to file their beneficial ownership information to TRA. The most common reason for rejection of the license is lack of necessary application documents and failure to meet the entry requirements for the profession.

Notaries

290. Notaries are appointed by the MoJ. The requirements for entering in the sector are strict and the notaries public are under the monitoring and supervision of the MoJ and the Union of Notaries Public of Türkiye. Accordingly, the Supervisory Board of the Union of Notaries Public of Türkiye supervises whether the notary chambers and notaries public carry out their duties in compliance with the laws, regulations, circulars and mandatory professional rules. The MoJ supervises all kinds of activities of the Union, the chambers and the notaries public as well as their accounts and transactions by employing judicial inspectors or public prosecutors. In this respect, notaries public are under constant supervision of public prosecutors and are subject to on-site inspections at least once a year. Notaries Public are required to file their beneficial ownership information to the TRA. The most common reason for rejection of the application is that the entry requirements for the profession have not been met. (notary public certificate with insufficient seniority).

4.1.2. Detecting and addressing breaches

291. Türkiye has detected unlicensed activities in relation to DNFBPs to some extent. As with FIs unlicensed activities (see IO.3), authorities demonstrated a co-ordinated approach combining preventive, supervisory, and enforcement actions, contributing positively to the effectiveness in detecting unlicensed activities. Identification is allowed through various channels such as denunciation mechanisms open to public, LEAs, tax inspections, notifications from other supervisory authorities, social media monitoring.

292. To ensure that complaints regarding natural or legal persons engaged in unlicensed DPMS and REAs activities can be made in a faster and in an easier manner, the MoT set up specific a reporting system. Complaints are examined directly by the Provincial Directorates of Trade, and inspections are conducted accordingly.

Table 4.1. Administrative fines for unauthorised DPMS and REAs activities

Year	Number of Persons Fined (REA)	Total Amount of Administrative Fine (EUR)-REAs	Number of Persons Fined (DPMS)	Total Amount of Administrative Fine (EUR)-DPMS
2021	329	198 054	-	-
2022	114	54 606	-	-
2023	1200	3 796 146	-	-
2024	572	1 318 824	125	700 000
2025*	625	1 959 706	93	419 700
Total	2 840	7 327 336	218	1 119 700

Note: *until 28 November 2025.

293. The persistence of a high number of unlicensed actors in the DPMS and REA sectors could reflect a lack of dissuasiveness of the sanctions allocated in those cases.

294. Monitoring of fit and proper requirements post licensing is ensured through supervisory activities. Those are conducted by the regional directorates of the Ministry of Trade for DPMS and REAs. Accountants and lawyers are monitored via their SRB while notaries are regularly inspected by the Ministry of Justice.

295. For accountants, the licenses of those found to have lost these conditions are revoked by decision of the Union Management Board. For example, the licenses of members who have been convicted of certain crimes, who have lost their legal capacity, or who are found to be in situations that are incompatible with the honour and dignity of the profession are revoked.

296. For lawyers, there are supervision and disciplinary mechanisms that operate ex officio, based on reports and complaints, regarding colleagues who commence and continue their legal practice. If a lawyer receives a license revocation penalty, all notaries are informed since the lawyer-client relationship is established through a power of attorney. In addition, since their e-signature authorisations have been revoked, they cannot use the UYAP system in any way and therefore cannot carry out duties as a lawyer. Over the reporting period, 17 licenses were suspended and 122 cancelled.

Table 4.2. Lawyers licenses suspended/cancelled

Year	Licences Suspended*	Licenses Cancelled
2020	0	9
2021	2	14
2022	5	40
2023	4	39
2024	4	14
2025	2	6

297. Notaries who act contrary to professional rules, perform their duties negligently, or engage in conduct that undermines public trust are subject to disciplinary proceedings. The possible sanctions range from warnings and reprimands to fines, temporary suspension, and revocation of the notary's license. License revocation effectively removes the notary's authority to perform notarial duties and permanently halts their official activities. 26 notaries have been dismissed from their profession in the period of 2022-2025. The cause of repeal is having lost the qualification to be a judge, prosecutor, civil servant, or lawyer as a result of a final criminal or disciplinary decision.

4.2. Supervisors identifying, understanding and promoting DNFBP understanding of ML/TF risks

4.2.1. Identifying and maintaining an understanding of the ML/TF risks in the different sectors and types of DNFBPs and of individual DNFBPs over time

298. Türkiye has largely identified and understood the ML/TF risks in the DNFBP sector through a comprehensive risk assessment. MASAK demonstrates a comprehensive understanding of ML/TF risks across the DNFBP sector. Sectoral supervisors' risk understanding is more limited and focuses more on risk mitigation measures than on actual ML/TF risks. Given MASAK's role as the primary AML/CFT supervisor, this difference in understanding is expected; however, enhancing sectoral supervisors' knowledge of ML/TF risks would improve their ability to carry out AML-related supervisory tasks effectively.

299. As described in IO.3, Threat and Vulnerability Working Groups were established in 2021 as a result of the adoption of the AML/CFT Strategy. Under the Threat & Vulnerability WG, 8 risk analysis sub-groups were created to assess sectoral risks and entities risk level including one for DNFBPs, focusing on DPMS, REAs and vehicles traders (those are outside the scope of the FATF Methodology, see IO.1). A methodology different than the one for FIs was used to assess the risk in of DPMS and REAs to take into consideration the specificities of those sectors such as the high number of entities, the absence of a professional association representing the entire sector, their limited products and services, the relatively recent AML/CFT requirements and limited awareness and the high level of unlicensed activities. The WG established comprehensive risk scenarios and took into consideration specific risk factors in each sector, allowing to group entities in risk levels groups and then calculating the final risk score for each entity. As a result, both DPMS and REAs sectors have been considered as medium-high risk.

300. Although lawyers, accountants and notaries have not been included in the risk analysis WG, a similar methodology has been used for analysing the risks in each sector. Risk analyses for accountants, notaries and lawyers are performed by MASAK with the support of related stakeholders by using past studies, experiences and professional expertise information. Several factors have been considered in the risk analyses of these sectors such as requirements for operating in the sector, supervision results, products and services, previous ML/TF abuses in the sector, STRs submitted- after assessing these factors, obliged parties with ML/TF risks were identified for each sector to constitute a basis for supervision of obligations. As a result, accountants have been classified as "medium", lawyers as "medium-low" and notaries as "low" in terms of ML/TF risks.

301. Entities risk rating in the entire DNFBP sector is reviewed annually and forms the basis for the establishment of risk-based supervision programs (see 4.5). Sectoral risks are reviewed annually for highest risk sectors (DPMS, REAs and accountants) as a basis of supervision programme and every two years for other sectors as part of the NRA process.

Table 4.3. DNFBP sectors risk level

Sector	Risk Level	Number of institutions	Number of high-medium risk (as of 2024)
DPMS	Medium-High	11 986	288
REA	Medium-High	77 831	182
Accountants	Medium	133 439	24
Lawyers	Medium-Low	199 142	80
Notaries	Low	2 383	-

4.2.2. Promoting DNFBP understanding of ML/TF risks and AML/CFT obligations

302. MASAK's activities have strengthened DNFBPs' understanding of ML/TF risks and their related obligations, with DNFBPs widely acknowledging the informative work conducted by MASAK. Professionals met during the onsite reported that they would benefit from further awareness raising sessions, especially on ML/TF typologies to better capture potential suspicious cases.

303. MASAK also published several guidance specifically for the DNFBP sector. These guidelines provide information on ML/TF risks, but also AML/CFT obligations of DNFBPs, including a specific guidance on combating TF for DNFBPs (2022) and a guidance on ML/TF obligations in the DNFBP sector (2025).

304. In addition, MASAK, in co-ordination with sectoral regulatory and supervisory authorities organised numerous workshops and trainings for all DNFBP sectors. Those also cover both understanding of risks and AML/CFT obligations. Through feedback obtained during those workshops, MASAK has updated its DNFBP sectoral guidance accordingly.

4.3. DNFBP understanding of existing and evolving ML/TF risks

305. Despite the positive steps taken by competent authorities and described above, DNFBPs' understanding of ML/TF risks remains limited. In the DPMS and REAs sectors, the understanding of ML risks is more developed, especially for larger entities. TF risk understanding is limited to awareness of TF related TFS obligations. Some DPMS and REAs, especially larger groups, met during the onsite visit had institutional risk assessment related to their customers, products/services, distribution channels and geographical risks.

306. Accountants, lawyers and notaries have a more limited understanding of ML/TF risks, mainly considering that their professions are largely prevented from those risks based on the strong requirements to become an accountant or a legal professional and of the knowledge they have of their clients. They also considered as a mitigating factor the fact that most transactions they are operating are going through the banking sector and rely on this sector for the detection of potential suspicious activity.

4.4. DNFBP understanding and compliance with AML/CFT obligations and mitigating measures

4.4.1. CDD, record-keeping, BO information, ongoing monitoring

307. Overall, DNFBPs apply CDD to some extent and have a basic understanding of BO requirements but rely too heavily on other reporting entities' AML/CFT obligations to mitigate risks.

308. CDD requirements are implemented across all sectors for any transaction above the legal threshold of approx. EUR 3 500, with certain accountant and legal professions applying CDD measures for any customer. DNFBPs also rely on official identification documents as part of CDD process and some entities reported their refusal to carry out a business relationship due to the inability to identify or verify the identity of the customer. However, violation of CDD requirements is the most common violation of AML/CFT requirements by DNFBPs and the ratio of entities that have been supervised and found in violation remains high, highlighting that the implementation of those requirements needs to be strengthened.

309. Many DPMS and REAs use a KYC form that includes all the criteria requested by law, and collect customer and beneficiary information through this way, but verification of the accuracy of the information is not always conducted. For REAs, an online system has been established by the MoT for the advertisement of real estate which requires, any person willing to buy/sell property via a REA to disclose identity information and provide relevant documentation.

310. Some entities have published their obligations regarding customer identification on their websites to give information to customers, including the need for those who act for the benefit of others to disclose it. Accountants, lawyers and notaries are by virtue of their activities more familiar with their clients and perform CDD at the onboarding stage. Nevertheless, DNFBPs conduct CDD monitoring to a more limited extent, mostly if a suspicion arises.

311. There is an overall understanding of the concept of BO in the DNFBP sector. Yet, DNFBPs largely rely on information provided by their clients to identify BO and report challenges to perform BO identification in the case of foreign legal persons. The ownership structure is only checked to some extent in accordance with the information held by the TRA through the tax statement that legal persons are asked to provide when entering into a business relationship. Some DNFBPs also conduct manual checks on open-source information if doubts arise. Notaries are performing public service duties and cannot carry out transactions within the scope of their authority (sales of assets, registration, company contracts, power of attorney) without BO verification.

312. As FIs, DNFBPs are required to retain the documents, books and records, identification documents kept in all forms regarding their transactions and obligations for eight years and provide all kinds of information and documents when requested by supervisors. Since the violation of this obligation will result in criminal charges and potential imprisonment up to three years there is general awareness on this requirement across DNFBPs. Since 2021, three criminal complaints were filled by supervisors to the public prosecutor's office for infringement with record-keeping requirements and two criminal complaints were filled for infringement with providing information requirements.

4.4.2. Enhanced or specific measures

313. DNFBPs met during the onsite generally perform EDD when considering high-risk clients and/or transactions. Criteria such as destination of the transaction, origin of wealth, use of cash, suspicion on client identity or ultimate beneficiary of the transaction. DNFBPs met during the onsite indicated that they would conduct EDD on customers from higher-risk jurisdictions, while some indicated that they would automatically reject customers from specific countries which could lead to disproportionate exclusion of some.

314. DNFBPs have an overall understanding of the concept of PEP but identification is achieved to a limited extent. Checks are mostly conducted manually and while larger DNFBPs resort to commercial databases, smaller entities rely on their own knowledge of the customer. Some DNFBPs reported that EDD could extend to PEP relatives when they are identified but reported challenges in identifying foreign PEP.

4.4.3. AML/CFT reporting obligations, tipping off

315. Except for DPMS, other DNFBP sectors barely report suspicious transactions, this is not in line with the risks they are exposed to especially for REAs, accountants and to a lesser extent lawyers.

316. In line with its 2020 ICRG Action Plan, Türkiye has strengthened awareness raising for DPMS and REAs in terms of suspicious reporting, including via the issuance of a specific guidance. This has led to a significant increase in the number of STRs, nevertheless, this increase is solely driven by the enhanced reporting of DPMS, while other sectors reporting remains negligeable. This coupled with the DNFBPs generally lower understanding of ML/TF risks, increase the risks of undetected suspicious activities. In addition, supervisors barely detect breaches of STRs reporting when conducting inspections of DPMS and REAs, which questions the effective monitoring of this criteria. DNFBPs met during the onsite reported that they would benefit from further understanding of ML/TF typologies to better capture potential suspicious cases.

317. DNFBPs are generally aware of the risk of tipping-off. To prevent potential tipping off, some entities conduct trainings to their personnel most involved in commercial relations, especially in the REAs and DPMS sectors.

Table 4.4. Suspicious reporting by DNFBPs

	2020	2021	2022	2023	2024	2025*
DPMS	51	138	320	683	1 097	2 161
REAs	-	9	2	19	1	6
Lawyers	-	2	-	3	3	-
Notaries	5	24	22	4	1	3
Accountants	-	-	-	-	-	42
Total	56	173	344	709	1 102	2 212

Note: *until November 2025.

4.4.4. Internal controls, procedures and audit to ensure compliance

318. Unlike FIs, DNFBPs are not obliged to prepare a compliance program but are required to carry out training, surveillance, monitoring and control activities to identify risks and take appropriate mitigating measures, in practice this is only done by larger DNFBPs. As described above, DNFBPs develop institutional risk assessment to a limited extent which does not support the implementation of effective internal controls and procedures to ensure compliance. In addition, supervisors almost did not identify infringement of internal controls requirements, indicating that there is a lack of focus on the implementation of such measures in the course of supervisory activities which is a concern.

319. Internal controls are generally established in larger DNFBPs with internal control processes and procedures specifically related to their business activities and designation of compliance officers. Some international firms (accounting, law, DPMS) apply group-wide AML/CFT controls.

4.4.5. Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

320. There are no legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures.

4.5. Supervisors risk-based monitoring or supervising compliance by DNFBPs

321. Türkiye follows a risk-based approach for the supervision of DNFBPs. Given the high number of DNFBPs in the country (more than 400 000), MASAK prioritises the supervision of high-risk entities within the highest risk sectors (DPMS, REAs and accountants to a lesser extent).

322. Similarly, as for FIs (see IO.3), as a result of its ICRG Action Plan, Türkiye adopted a risk-based supervision approach in 2021 to prioritise the supervision of highest risk sectors and highest risk entities within those sectors. MASAK, as the main AML/CFT supervisor, prepares annual supervision plans for DNFBP sectors presenting the highest risks (DPMS, REAs and accountants). The Threat & Vulnerability WG and the DNFBP risk WGs provides a platform for MASAK to exchange with sectoral supervisors as well as the private sector and the development of the sectoral risk assessments support the definition of yearly supervisory programs. Türkiye's RBS methodology requires obliged entities categorised as high-risk to be supervised every year, and obliged entities categorised as medium risk to be supervised every three years at the latest.

323. Supervision programs are carried out either by MASAK or sectoral supervisors under MASAK's oversight. Dedicated protocols between MASAK, MoT and TIB were signed to enhance co-operation and co-ordination and ensure that supervisions will be performed with a risk-based approach and ML/TF risk understanding of supervisors will improve. They also set forth the duties and responsibilities of the institutions on exchange of information, on trainings and on organising workshops with the participation of professional associations. All the supervisory authorities prepared RBS guidance to ensure that their own supervisions, within the scope of their regulatory laws, are performed by taking ML/TF risks into consideration.

324. On that basis, supervision of DNFBPs follows an integrated approach. First, dedicated AML/CFT supervision programmes defined yearly by MASAK are conducted either by MASAK or sectoral supervisors under MASAK's guidance. Those onsite inspections aim at assessing the compliance status of the reporting entity against AML/CFT obligations. Second, sector specific/operational supervision conducted by sectoral supervisors. Those are not targeted at AML/CFT obligations but if related shortcomings is identified by the sectoral supervisor (e.g. CDD requirements, BO, etc.) the case is referred to MASAK for further examination.

Third, "case-based AML/CFT inspections", if there is a suspicion of a violation outside the scope of pre-planned activities. As a result, all high-risk entities in the DPMS, REAs and accountants sectors are supervised yearly and medium risk ones have been supervised at least once over a three-year period.

325. However, the effectiveness of supervisory measures is limited by some weaknesses. MASAK supervisory staff is somewhat limited, and sectoral supervisors monitor AML/CFT obligations to a lesser extent. In line with its ICRG Action Plan, MASAK's resources dedicated to supervision have been strengthened since the 2019 MER, from 12 staff members to 33 as of 2025. Nevertheless, MASAK supervision department oversees compliance for all reporting entities (FIs, VASPs and DNFBPs) and receives and analyses the reports of all sectoral supervisors, and is in charge of taking further actions, including issuing sanctions and conducting onsite inspections. Even though MASAK relies on sectoral supervisors, those do not have dedicated AML/CFT units nor specialised staff. In addition, while sectoral supervisors have a larger amount of resources to carry out inspections, their understanding of ML/TF risks in the DNFBP sector is limited which does not ensure their full ability to identify the full scope of potential AML/CFT obligations beyond basic ones. In light of MASAK's broad prerogatives and pivotal role it plays to conduct and co-ordinate AML/CFT supervision, its resources for supervision still need to be further strengthened. This coupled with DNFBP sectoral supervisors limited ML/TF expertise, hinders the effective supervision of the DNFBP sector.

326. In addition, the number of supervisory activities conducted over the reporting period is marginal in comparison with the size of the sector. The overall low number of entities supervised in the DPMS and REAs sectors is mostly in line with the low number of entities identified as high/medium risk in those sectors. Yet, in 2024 the number of entities supervised in both sectors amount to approx. 0,2% of the overall number of entities in those sectors. Based on the risks those sectors are exposed to, the fact that some sectors (i.e. lawyers) have been recently subjected to AML/CFT obligations and their overall low-level awareness of those requirements, supervisory activities remain marginal to enhance compliance across those sectors. Supervisors could rely to a larger extent on a mix of onsite and offsite supervision activities which would allow to broaden the scope of reporting entities monitored on the basis of their AML/CFT obligations.

327. Sectors considered as presenting a medium risk (accountants) or medium-low risk (lawyers), received marginal supervision over the reporting period, while no supervisory activities were conducted for notaries. Based on the types of activities performed by those sectors, especially support to the creation and management of legal persons and registration of transactions, supervision for those sectors is not in line with the risks they are exposed to. These challenges suggest that the effectiveness of the risk-based supervision in the DNFBP sector is only achieved to some extent.

Table 4.5. Supervision of DNFBPs

Sectors	Number of entities (as of 2024)	2021		2022		2023		2024		Total	
		High/Med risk	Supervised	High/Med risk	Supervised	High/Med risk	Supervised	High/Med risk	Supervised	High/Med risk	Supervised
REAs	77 831	96	53	549	100	131	109	182	98	958	360
DPMS	11 986	98	51	1 869	100	301	120	288	105	2 556	376
Accountants	133 439	15	5	0	0	32	15	24	11	71	31
Lawyers*	199 142	0	-	0	-	80	8	0	-*	80	8
Notaries	2 383	0	-	0	-	-	-	0	-	0	-
Total	424 781	209	109	2 418	200	544	252	494	214	3 665	775

Note: *Lawyers could not be included in the supervision programme in 2024 due to the Constitutional Court's decision annulling their designation as an obliged party (Official Gazette 32509, dated 03.04.2024).

4.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate and dissuasive sanctions on DNFBP compliance

328. MASAK has implemented some remedial actions and has imposed fines for non-compliance with CDD measures to some extent and suspicious reporting to a limited extent, but an overall positive impact from such measures has yet to be demonstrated.

329. Supervisors have a range of administrative sanctions available, with flexibility on the monetary amount depending on the severity of the breaches. In line with Türkiye's ICRG Action plan, the amount of administrative fines has increased since 2021 but remain relatively low for breaches of AML/CFT obligations. This amount is reviewed on a yearly basis according to the revaluation rate in order not to lose value due to inflation and in accordance with the Tax Procedure Law.

Table 4.6. Applicable administrative fines for DNFBPs

Obligation	Applicable Administrative Fine Amounts (EUR)					
	2020	2021	2022	2023	2024	2025
CDD	3600	3 175	2 541	4 075	4 410	4 987
STR	6000	5 292	4 235	6 791	7 349	8311
Periodic Reporting	3600	3 175	2 541	4 075	4 407	4 987
Max Amounts	480 000	449 537	338 826	502 318	587 960	664 911

330. When criminal offences are detected, MASAK files a criminal complaint to the public prosecutor and can in parallel suspend the reporting entity. Over the reporting period, MASAK has filled 3 criminal complaints against DNFBPs for record keeping infringement and 2 criminal complaints for violation of providing information requirement.

331. Over the reporting period, in line with the RBS undertaken with a focus on DPMS and REAs, representing the highest risk sectors, AML/CFT violations have mainly been detected mostly for those two sectors. Except in nine cases, all other violations are related to shortcomings on CDD. Supervision and remedial actions are mainly undertaken on CDD requirements, which limits the effectiveness of supervisory activities to improve overall compliance with all AML/CFT obligations. This is a concern especially for STRs reporting where the overall reporting of suspicious activities remain low, except for DPMS, but supervisors do not identify breaches of those obligations which could indicate a limited focus on this requirement during the course of supervisory inspections.

332. When shortcomings are identified, entities are prioritised to be subjected to a supervision programme the following year to monitor that deficiencies have been addressed. Yet, in light of the persistence of a high rate of supervised reporting entity found to be in violations with CDD requirements, remedial actions and sanctions can only be considered effective to a limited extent, and sanctions imposed not sufficiently dissuasive to foster compliance.

333. The limited remedial actions and sanctions applied against accountants and legal professionals is in line with the lower focus of the supervisors on those sectors. However, in light of the limited understanding of the professionals met during the onsite visit on ML/TF risks related obligations, further identification of higher risk entities and supervision of those are needed.

Table 4.7. Sanctions against DNFBPs on AML/CFT breaches

Sectors	2021			2022			2023			2024		
	Supervised	Violations	Fines (EUR *1 000)	Supervised	Violations	Fines (EUR *1 000)	Supervised	Violations	Fines (EUR *1 000)	Supervised	Violations	Fines (EUR *1 000)
REAs	53	29	735	100	57	492	109	37	413	98	41	759
DPMS	51	43	1364	100	78	954	120	93	2065	105	45	1076
Accountants	5	0	-	0			15	8	101	11	4	24
Lawyers	-			-			8	3	15	-	-	
Notaries	-			-			-			-		

334. MASAK does not publish enforcement actions but it communicates annually through its activity report and during the course of its outreach activities to each sector on the main regulatory breaches. However, entities met during the onsite visit had limited knowledge of the most common breaches in their sector and further awareness raising from MASAK would be beneficial.

335. Over the reporting period, MASAK has undertaken significant efforts to increase DNFBPs' understanding of their AML/CFT obligations with the issuance of dedicated guidance and the conduct of numerous trainings for all sectors. Some professionals met during the onsite visit also considered that MASAK's inspections were beneficial and informative as they did not only focus on identifying shortcomings, but supervisors also take the time to train and explain obligations to reporting entities' staff. Those activities are having a positive, yet still limited, impact on DNFBPs' compliance.

Box 4.1. Outcomes of supervision programmes and enforcement actions

DPMS A was included in the 2023 supervision programme, and it has been determined that, DPMS A had 23 violations, and it was imposed an administrative fine of approx. EUR 37 000. Based on those shortcomings, in 2024 DPMS A was again included in the supervision programme, and it has been determined DPMS A still had 10 violations, and it was imposed an administrative fine of approx. EUR 20 000.

REA Y was included in the 2022 supervision programme, and it has been determined that, it had 29 violations and it was imposed an administrative fine of approx. EUR 23 000. In 2024, REA Y was included in the supervision programme again and it has been determined That it had 3 violations and was imposed an administrative fine of approx. EUR 6 000.

5 Transparency and beneficial ownership

The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this chapter are R.24-25 and elements of R.1, 10, 22, 37 and 40.[27]

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Turkish authorities demonstrate a generally good and evolving understanding of ML/TF risks associated with domestic legal persons created in Türkiye. This understanding is supported by the NRA, the 2021 and 2025 LPRA, and by strong operational insights held by MASAK and LEAs. Legal persons are recognised as being primarily misused in complex ML schemes. However, this operational understanding is not yet fully reflected in formal risk assessments, and this level of nuance is not fully captured in the LPRA, which presents an overall rating and does not explicitly reflect the differentiated risk landscape and use cases. As a result, the risk picture is more complex than suggested by the overall risk characterisation of the LPRA, and this may limit the consistent communication of these insights across competent authorities and reporting entities.

b) Türkiye has taken meaningful steps to assess risks related to foreign-created legal persons with sufficient links. But the analysis requires additional calibration, and the understanding of these risks remains less developed, and is uneven across competent authorities and obliged entities. The understanding of risks associated with foreign legal arrangements remains limited and focused on their operational absence domestically rather than their potential use in practice. TF risks are broadly identified and generally developed; however, they are not sufficiently differentiated between domestic and foreign legal persons, limiting a coherent and granular understanding of risk.

c) Türkiye has established clear transparency controls for basic information on commercial legal persons through the Trade Registry and MERSIS, supported by notarial involvement at key corporate events, which ensure formal legal compliance and traceability of legal ownership. Türkiye also applies robust monitoring and enforcement measures for associations and

[27] The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

foundations through the DERBIS and VBYS systems, which are aligned with identified risks and contribute to preventing misuse. However, for commercial legal persons, controls are primarily focused on formal requirements and do not extend to substantive AML/CFT verification, limiting their effectiveness in detecting misuse.

d) Türkiye applies comprehensive CDD obligations across financial institutions, VASPs and DNFBPs, which support the identification of BO and monitoring of customer relationships. However, their effectiveness is constrained by a sanctions framework that is not fully dissuasive for non-compliance, and an uneven understanding of ML/TF risks among reporting entities. While understanding appears stronger among banks, it is more uneven across other parts of the financial sector, including certain VASPs and capital market participants, and is weakest among DNFPBs.

e) Türkiye actively applies measures to address dormant companies, including the systematic striking off of inactive entities, which contributes to a good extent to mitigate risks associated with legal persons. However, there is no evidence that complementary measures have been undertaken to target the directors, shareholders or beneficial owners behind these entities, when involved in ML/TF activity, and the underlying risk may therefore persist, as the same individuals can continue to establish new legal persons, including in typologies involving shell and front companies, a recognised typology in Türkiye.

f) Türkiye's framework for collecting BO information based on a multi-pronged approach is comprehensive, drawing on the BO Registry maintained by the TRA, information collected by obliged entities through CDD measures, Trade Registry Gazette and MERSIS, Central Securities Depository (MKK) records, and cross-checking mechanisms through MASAK databases and audits. These sources enable competent authorities, notably MASAK and LEAs, to access structured ownership and control information in a generally timely manner. However, in practice there is a concentrated reliance on the BO Registry and MERSIS, with more limited use of other available sources, and no evidence of use of the BO Registry, by other competent authorities reducing the extent to which the full benefits of the multi-pronged framework are leveraged.

g) Türkiye does not yet have sufficiently systematic and risk-based mechanisms to ensure that the information contained in basic and beneficial ownership registers is consistently accurate and up to date. Verification measures to the BO Registry are applied through targeted cross-checks and inspections, and to some extent, provide a baseline level of assurance and have identified inconsistencies; however, these remain largely ad hoc and require greater depth of verification, particularly for higher-risk domestic and foreign-created legal persons, limiting the overall reliability of BO information.

h) Türkiye has strengthened its sanctions framework for breaches of basic and BO obligations and demonstrates active enforcement, particularly through administrative fines linked to BO reporting, contributing to high levels of formal compliance. However, enforcement is more limited in higher-risk areas, particularly for commercial legal persons registered through the MERSIS system, with limited action against fraudulent companies, violations of the TCC, and foreign-created legal persons with sufficient links. In addition, penalties for bearer share breaches remain modest, and the absence of criminal liability for legal persons increases reliance on administrative measures, limiting the overall deterrent effect, particularly in more complex ML/TF scenarios.

Key Recommended Actions (KRAs)

Türkiye should:

j) Enhance the understanding of ML/TF risks associated with foreign – created legal persons with sufficient links, by refining the criteria used to define sufficient links on a risk basis, improving alignment between risk assessments and typology materials and developing a more differentiated understanding of TF risks across domestic and foreign-created legal persons, particularly in cross-border contexts and ensure that operational insights on domestic legal persons are more explicitly reflected in formal risk assessments.

k) Strengthen the use of the Trade Registry and MERSIS as active ML/TF mitigation tools throughout the lifecycle of legal persons, including at incorporation, to detect inconsistencies and enhance overall effectiveness while supporting risk management.

l) Prioritise more comprehensive, risk-based verification mechanisms to ensure that BO information is accurate and up to date. This may include strengthening verification of both the identity of the beneficial owner and whether the identified individual is in fact the true beneficial owner, alongside enhancing the filing and processing of discrepancy reports submitted by obliged entities and increasing the routine use of BO registry data by competent authorities beyond law enforcement.

Other Recommended Actions

Türkiye should:

a) Implement targeted outreach and training to DNFBPs and other obliged entities on areas of weaker understanding, including effective identification of beneficial ownership in complex cross-border structures.

b) Strengthen the deterrent impact of the sanctions regime by enhancing the use of existing administrative measures across higher-risk legal persons, including TCC violations, fraudulent companies and foreign-created legal persons with sufficient links

c) Deepen qualitative understanding of ML/TF risks associated with foreign legal arrangements with sufficient links to Türkiye, including by analysing their use in complex ownership structures, cross-border investment, including real estate and asset management contexts.

d) Enhance disaggregated data collection and analysis of domestic legal persons and foreign-created legal persons with sufficient links, to support more granular risk assessment and strengthen oversight of the effectiveness of preventive, supervisory and enforcement measures.

e) Develop alternative approaches within the administrative sanctions framework to address more complex or serious cases involving legal persons, in the absence of criminal liability for legal persons.

Overall Conclusions on IO.5

Türkiye has identified and assessed the main ML risks associated with domestically created legal persons, supported by the NRA, successive LPRA and demonstrated strong operational understanding within MASAK and LEAs. This understanding provides a solid foundation, although it is not yet consistently reflected across all competent authorities. Legal persons are recognised as being primarily misused in complex ML schemes. The understanding of TF risks, including risks identified in relation to specific actors, cross-border financial flows and the use of legal persons and commercial structures to facilitate such activity, is established but remains broad and lacks sufficient differentiation across types of legal persons, including between domestic and foreign-created legal persons. The understanding of risks associated with foreign-created legal persons and foreign legal arrangements with sufficient links to Türkiye remains less developed. In particular, reliance on a singular threshold-based approach for foreign created legal persons that are not limited taxpayers (e.g. 50% ownership) limits the ability to capture more complex ownership and control structures. For legal arrangements, the analysis does not sufficiently consider, from a qualitative perspective, how these structures may be misused, particularly when they are layered within other legal structures (e.g. trusts embedded within corporate ownership chains), or own or control a domestic legal person, resulting in a more general articulation of risk.

Türkiye has made significant progress in strengthening the framework for transparency and reducing opportunities for anonymity. Measures are in place to prevent misuse, including transparency requirements through the Trade Registry, public availability of basic information, BO reporting obligations, controls on bearer shares and the non-recognition of nominee director and shareholder regimes. BO information is available to competent authorities, with examples indicating generally timely access, particularly for law enforcement. Compliance with reporting obligations across legal persons is high, and initial verification efforts, including cross-checks and data-matching exercises, provide, to some extent, a useful baseline of assurance. At the same time, these measures do not fully ensure that the information is accurate and up to date. In particular, the accuracy of basic information in the Trade Registry and MERSIS relies to a large extent on self-reported data and formal checks, with limited evidence of substantive verification. Similarly, while BO verification mechanisms exist, they remain largely ad hoc and not as in-depth, which limits assurance that BO information is consistently accurate and up to date. The use of such information by competent authorities' other non-law-enforcement authorities is also less developed in practice.

Türkiye has strengthened its sanctions framework and demonstrates active use of administrative measures in several areas. Nonetheless, the application of sanctions could be further enhanced to ensure that they are consistently aligned with the scale and nature of risks, particularly in relation to higher-risk legal persons, fraudulent companies and foreign-created legal persons with sufficient links.

Outcome is achieved to some extent, and major improvements are required.

Türkiye is rated as having a Moderate level of effectiveness for IO.5.

Immediate Outcome 5

336. Türkiye is not considered a company or trust formation centre and does not exhibit features typically associated with jurisdictions that specialise in the mass incorporation of legal persons or arrangements. Both the NRA and LPRA explicitly acknowledge that legal persons are used in ML/TF schemes, often through front and shell companies to disguise ownership and transactions, thereby

facilitating the placement, layering and concealment of illicit proceeds, while overall risk remains limited and concentrated in specific risk types and sectors. The types of companies in Türkiye are detailed in Table 5.1. The materiality of legal persons is concentrated overwhelmingly in capital companies—particularly limited and joint stock companies—which account for the vast majority of entities and economic activity, with limited companies alone representing over 80% of all companies. As reflected in the LPRA and NRA, these entities constitute key vehicles through which ML/TF risks may materialise, reflecting their scale, operational flexibility and engagement in domestic and cross-border transactions. Joint stock companies tend to present relatively higher risks, including in relation to BO complexity and their greater exposure to foreign and domestic trade, while limited companies reflect risk through their volume and widespread use across sectors, including in cash-intensive and transactional activities. Other legal persons, such as co-operatives, associations, foundation enterprises and partnerships, are significantly less material in both number and impact, generally exhibiting more contained risk profiles, although certain categories (e.g. associations) remain relevant in the context of TF. Foreign legal persons with sufficient links—such as limited taxpayer entities (e.g. branches) and companies with significant foreign ownership—form a smaller but relevant subset, with risk exposure that differs in nature rather than scale, particularly in relation to BO transparency and cross-border activity, consistent with the LPRA's identification of inherent risks linked to foreign ownership and transactions.

337. At the same time, Türkiye's economic structure—as a trade- and transit-oriented economy with significant cross-border flows—adds an additional layer of complexity to this risk environment. The NRA highlights the role of international trade, smuggling routes and cross-border financial movements as central risk drivers, including the use of companies to facilitate financial flows under the appearance of legitimate trade and to support trade-based money laundering and terrorist financing schemes. In parallel, real estate remains a relevant channel for the integration of proceeds of crime, reflecting its role in absorbing illicit funds within the domestic economy. Investment activity has also expanded, including a reported 114% increase in fund size between 2024 and 2025, alongside a substantial rise in the number of funds (424 new funds). This reflects the growing role of investment vehicles, financial intermediation, and capital market structures in Türkiye's financial system. This is complemented by continued inflows of foreign capital, with Türkiye attracting USD 13.1 billion in foreign direct investment in 2025, representing a 12.2% year-on-year increase, with a significant share directed toward trade, manufacturing and technology sectors. While these developments reflect economic dynamism, they also introduce additional layers between investors and underlying assets and increase the scale and cross-border nature of financial activity. Taken together, the risk landscape is shaped not only by the legal form of entities, but by their economic function, their role in trade and transit activities, and their integration into financial and real estate markets, which collectively influence how ML/TF risks materialise in practice.

Table 5.1. Types of companies in Türkiye

Type of Company	2020	2021	2022	2023	2024	2025*
Joint Stock Company	142249	158097	178091	197976	215098	223915
Limited Company	859570	958218	1083805	1204586	1314337	1388132
Joint Ventures	1083	1210	1372	1627	1864	2108
Association Enterprise	2707	2799	2916	3016	3047	3098
Foundation Enterprise	962	957	978	990	1002	981
Collective Company	10876	10732	10667	11145	11106	11047
Commandite	2031	2024	2023	2023	2020	1988
Co-operative	48954	49436	50317	52605	54439	49864
TOTAL	**1068432**	**1183473**	**1330169**	**1473968**	**1602913**	**1681133**

Note: (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025);

5.1. Identifying, assessing and understanding ML/TF risks of legal persons and arrangements

5.1.1. Turkish Legal Persons

338. Türkiye demonstrates a generally good and evolving understanding of ML/TF risks associated with legal persons created in the country. This understanding is grounded in the NRA and the LPRA conducted in 2021 and updated in 2025. The LPRA applies a structured methodology based on indicators relating to legal form, sectoral activity, transactional behaviour, geographic exposure and ownership characteristics. The 2025 update reflects methodological refinement with expanded indicators and increased use of tax, supervisory and law-enforcement data, contributing to a more differentiated assessment of domestic risks and providing a common analytical reference point for competent authorities. Competent authorities considered a wide range of sources in the formation of the LPRA.

339. The LPRA differentiates risks by company type and sector, identifying joint stock companies and limited liability companies as posing higher inherent risk due to their prevalence, transactional capacity, and suitability for layered ownership and control structures. It further identifies vulnerabilities in cash-intensive and trade-oriented sectors, including wholesale and retail trade, logistics and real estate. These conclusions broadly align with STR trends and domestic case experience, indicating that the formal risk assessment reflects the main channels through which domestically created legal persons are misused for ML purposes.

340. The understanding of TF risks associated with legal persons is established but remains broad and would benefit from greater precision and differentiation. The NRA, supported to a more limited extent by the LPRA, identifies TF risks as concentrated in specific actors, sectors and cross-border channels, while recognising vulnerabilities linked to cash-intensive activity, informal transfer mechanisms and the use of legal persons and commercial structures to facilitate financial flows, including in cross-border contexts and in proximity to conflict zones. However, the articulation of these risks remains largely at a general level and is not sufficiently or systematically differentiated across types of legal persons. In particular, the analysis does not adequately distinguish between domestic and foreign legal persons in the context of TF risk and would benefit from a more granular assessment of how TF risks may manifest across different legal forms and structures, including in harder to detect trade-exposed and cross-border sectors.

5.1.2. Foreign Created Legal Persons

341. Türkiye has taken meaningful steps to identify and assess risks related to foreign-created legal persons with sufficient links; however, some limitations remain in the scope and calibration of the framework, particularly in how sufficiency thresholds are applied across different higher-risk sectors identified or complex ownership structures in the LPRA, including trade-related activities, logistics and real estate, in light of the country's risk and context. Understanding of ML/TF risks associated with foreign-created legal persons with sufficient links to Türkiye is less developed amongst both authorities and obliged entities.

342. Türkiye identifies certain foreign-created legal persons as limited taxpayers where they derive income from sources in Türkiye, typically through a permanent establishment, branch, agency or other taxable presence under domestic tax legislation. For the period 2021–2024, 388 limited taxpayer companies were identified within the scope of the legal person risk analysis. This dataset reflects foreign legal persons that have a recognised taxable presence in Türkiye. To widen the scope of analysis, MASAK also included 84 189 commercial companies with more than 50% foreign ownership. Within these datasets, 345 of the 388 limited taxpayer companies and 76 028 of the 84 189 companies with more than 50% foreign

ownership were identified as holding bank accounts in Türkiye, indicating financial linkages to the jurisdiction.

343. Legal persons with more than 50% foreign ownership interests represent 5.3% of all corporate taxpayers (9.4% of all corporate taxpayers is representative of companies that have at least 1 foreign shareholder). Methodologically, this approach potentially restricts the aperture of risk, as other than limited taxpayer status, it focuses on shareholding as a main criterion to determine sufficient link. The basis for considering the 50% threshold as an appropriate proxy for sufficient link, in light of Türkiye's risk and threat context, was not clearly elaborated, nor to what extent this approach may leave certain risks outside the scope of analysis. Authorities did not appear to consider whether differentiated thresholds or criteria may be warranted in higher-risk sectors identified in the LPRA or in light of Türkiye's exposure to cross-border activity, including where ownership structures are more complex or involve multiple layers across jurisdictions. In particular, the use of a single threshold may not fully capture risks in sectors or structures where lower ownership stakes or other forms of control may be sufficient to conceal BO. Given Türkiye's open investment climate and exposure to cross-border activity, exploring whether a more differentiated approach—particularly in higher-risk sectors or areas identified in the LPRA—would better capture these risks and could further support a more comprehensive understanding.

344. The LPRA defines foreign-linked entities through structural criteria such as tax presence and majority foreign ownership. The typology guidance—intended to support and deepen this understanding—does not reflect or operationalise these categories. Instead, it illustrates the use of legal persons in ML/TF schemes based on their functional role in cross-border activities, without linking these patterns to the LPRA's framework. For instance, typology material provides some evidence of the use of foreign legal persons and cross-border corporate structures, with such elements featuring in approximately one-third of the ML cases reviewed; however, these examples predominantly involve companies incorporated abroad or offshore entities used in multi-jurisdictional structures that do not satisfy the country's tests for sufficient link. No examples were identified that correspond to limited taxpayers or commercial companies with more than 50% foreign shareholding. For TF cases, typology material provides limited examples of foreign legal persons, with only one or two cases across the sample involving companies established abroad or foreign-controlled structures with a discernible link to Türkiye, primarily through fund transfers or organisational networks. As the typology guidance is a key tool through which the authorities communicate risk understanding, this indicates a disconnect between the risks observed in practice and the analytical framework applied, constraining the overall understanding of foreign-created legal persons with sufficient links.

345. MASAK and LEAs demonstrate a strong operational understanding of how corporate structures are misused in practice, notably in complex ML investigations. However, this level of operational insight is not consistently reflected across all other parts of the government, where understanding of risks appears more uneven, including among tax, company registry and supervisory authorities. MASAK consistently observed that legal persons are primarily exploited within complex ML schemes, including those involving multiple interposed entities, opaque ownership chains and the integration of illicit proceeds through seemingly legitimate commercial activity. This operational insight informs investigative prioritisation and analytical work. However, this understanding is not explicitly reflected in the LPRA narrative, limiting the extent to which these insights are institutionalised and systematically communicated across all competent authorities and reporting entities. Furthermore, this understanding is not reflected to the same degree across the private sector. While a basic understanding of BO risks is generally present, banks tend to demonstrate a stronger grasp of ML/TF risks overall. By contrast, the level of understanding is more uneven among DNFBPs and parts of the wider financial sector, including certain VASPs and capital market participants. In these sectors, awareness of risks—especially those involving complex ownership structures, cross-border elements or the misuse of legal arrangements—appears less developed and less consistently translated into practice.

5.1.3. Trusts and Foreign Created Legal Arrangements

346. Türkiye's overall understanding of risks related to trusts and foreign legal arrangements is partial. Authorities demonstrate strong awareness of risks where such structures are directly customer-facing, supported by outreach to obliged entities and targeted analysis. However, this understanding is more limited where such arrangements are embedded within layered, indirect or cross-border ownership structures, and is not yet fully developed in terms of identification, assessment and analysis of these more complex risks. Türkiye does not recognise trusts or equivalent domestic legal arrangements and authorities have substantiated the absence of such structures through legal analysis and empirical checks of registries, tax records and supervisory information. This position is appropriately reflected in the LPRA, when read in conjunction with the NRA. This does not preclude their use through cross-border arrangements. Under Turkish law, a person domiciled in Türkiye may act as settlor or beneficiary of a trust governed by foreign law, and foreign legal arrangements may operate in Türkiye, including through ownership or control of Turkish legal entities. The assessment of legal arrangement risks in the 2025 LPRA remains relatively narrow and concludes that risks related to trusts and similar legal arrangements are low, primarily based on the absence of formally identifiable trust structures. The analysis included outreach to obliged entities, including FIs, which identified a limited number of cases (e.g. 15 foreign start-up companies linked to investment fund structures). These were examined and excluded from the scope of trusts, as they did not exhibit the defining structural features of trust arrangements and were instead assessed as regulated investment relationships. Investment funds and family foundations were similarly excluded based on their legal form and regulatory framework.

347. However, the assessment focuses primarily on whether structures formally qualify as trusts and does not sufficiently analyse how foreign legal arrangements may be used in practice. While the authorities have made efforts to raise awareness—including issuing guidance and conducting training for obliged entities—these efforts are limited by the prevailing view that trusts are not present in Türkiye. In addition, no typologies or case-based examples are presented to illustrate how such arrangements could be used, particularly in layered or cross-border structures. Given that trusts are not a familiar legal concept in the jurisdiction, this creates challenges in identifying and assessing related risks. The AT is of the view that this gap, while present, is of lesser materiality given that foreign legal arrangements are not directly established or operating within the jurisdiction. Nevertheless, the absence of basic awareness remains a vulnerability that warrants attention, particularly in the context of cross-border layering typologies and Türkiye's role as a growing investment hub and recognised real estate investment hub.

348. Potential exposure through foreign legal arrangements—such as cross-border investment vehicles including for real estate, asset-management structures and arrangements involving intermediary jurisdictions—is not comprehensively integrated into the risk analysis. This gap in identifying, analysing and understanding is consistently reflected in discussions with both competent authorities and obliged entities. A recurring misconception is that the absence of domestic recognition of trusts or similar legal arrangements precludes their use as a layering vehicle in money laundering typologies. Obliged entities – notably legal professionals – demonstrated limited awareness of how BO transparency obligations required them to look through legal arrangements to identify the beneficial owner, of the circumstances under which such arrangements may be deliberately exploited to obscure the origin, movement or control of illicit finds. Overall, Türkiye's understanding of ML/TF risks associated with domestically created legal persons is sound and continues to improve, particularly at the operational level. Gaps in the depth and formalisation of analysis relating to foreign-created legal persons and foreign legal arrangements reduce the extent to which risk understanding is comprehensive, forward-looking and uniformly shared, with implications for the consistency of preventive and supervisory responses. Awareness of risks linked to foreign-created legal persons and foreign legal arrangements is more limited, particularly among DNFBPs. Banks tend to have a more sophisticated understanding, while other FIs and DNFBPs show weaker and more uneven awareness, reducing the effectiveness of mitigation measures in identifying complex misuse

typologies in practice. A similar pattern is observed in the understanding of TF risks, where the analysis does not adequately distinguish between domestic and foreign-created legal persons and remains insufficiently granular to capture how such risks may manifest across different structures, particularly in cross-border contexts.

5.2. Mitigating measures preventing misuse of legal persons and arrangements

349. Türkiye has implemented a broad range of preventive and mitigating measures aimed at reducing the misuse of legal persons for ML/TF purposes. These measures are grounded in company law, AML/CFT legislation, tax law and sectoral supervisory frameworks and apply throughout the existence of legal persons. Responsibilities are distributed across several competent authorities, with MASAK playing a central co-ordinating role in relation to AML/CFT obligations. While the framework is comprehensive and has strengthened transparency—particularly through incorporation controls and the BO Registry—its effectiveness is uneven in practice, with limited evidence of the detection of breaches of basic information related to commercial legal persons, reliance on self-reported information, and gaps in verification, enforcement and coverage across higher-risk areas, including joint stock and limited liability companies and foreign created legal persons with sufficient links.

350. Incorporation and Customer Onboarding: At incorporation and customer onboarding stage in Türkiye, a range of company law, tax, banking and AML/CFT controls on obliged entities apply to promote transparency to mitigate the misuse of all legal persons. Legal persons must register with the Trade Registry under the Turkish Commercial Code No. 6102 (and the Co-operatives Law No. 1163, where applicable), with incorporation information recorded and publicly disclosed through the Turkish Trade Registry Gazette and accessible via the MERSIS system. Newly established entities must submit a commencement of business notification to the tax authorities under the Tax Procedure Law No. 213, and trade registry directorates transmit incorporation documentation to the tax office via web service to enable cross-checks and address verification, including start-up inspections where the address information and submitted documents cannot be confirmed, along with additional safeguards for high-risk taxpayers (including collateral requirements in relevant cases).

351. CDD controls also operate as an early gatekeeper: obliged entities conduct CDD and identify BOs at account opening under the Regulation on Measures (RoM). In addition, these controls apply across all financial institutions (FIs) and DNFPBs. As part of their AML/CFT obligations, obliged entities are required to collect, maintain and update relevant customer and BO information, and to make this information available to competent authorities upon request. Türkiye has however not provided information on the number of such requests by competent authorities, their frequency and the timelines for provision of said information. Sanctions are imposed for non-compliance, but these are not proportionate or dissuasive in view of Türkiye's risk and context (See 5.5, IO.3 and IO.4).

352. Transparency of basic legal person information at the time of incorporation and through the life cycle of commercial legal persons is ensured through the Trade Registry and MERSIS systems, with public disclosure via the Trade Registry Gazette. Legal persons are required to register directors, shareholders and changes in ownership and management, without exemptions. These measures are intended to provide a transparent baseline and facilitate access to information by competent authorities and obliged entities. In practice, they are meant to constitute important mitigation measures against the misuse of legal persons for ML/TF purposes, particularly by supporting traceability of legal ownership and corporate changes. However, their effectiveness appears mixed, as they primarily capture formal legal ownership and rely on self-reported information, with checks focused on formal compliance rather than substantive verification. While penalties are applied where discrepancies are identified through complaints or audits, there is limited evidence of such checks and enforcement in practice, and none has been demonstrated in relation to

foreign legal persons. Article 210/3 of the TCC allows the Ministry of Trade to seek the dissolution of companies involved in fraudulent or unlawful activities; however, its use has been limited—applied to only 4 companies in 2021, 2 in 2022, 4 in 2023, 3 in 2024, and 5 in 2025. Given the use of multi-layered ML/TF schemes that feature shell and front companies and TBML laundering schemes, the application is not in line with the risk and context of Türkiye, particularly where the LPRA identifies joint stock and limited liability companies—those most commonly used in such structures—as posing higher inherent risks. This also underscores the limited evidence of detection at the point of incorporation and early-stage controls, with available data focusing primarily on limited ex post enforcement actions.

353. While this framework establishes multiple controls at the incorporation stage, only three cases – one initiated by the supervisory authority and two through complaints (**Box 5.1 refers**) were provided to demonstrate how Trade Registry and tax-level controls have, in practice, led to the identification of inaccuracies, corrective actions, sanctions or the detection and prevention of misuse of legal persons at the company law or tax levels. This is notably limited in light of Türkiye's risk and context, particularly given the concentration of legal person risks among commercial companies and the identified vulnerabilities associated with both domestic and foreign-created legal persons.

Box 5.1. Corrective Action against a company

In a notification sent by the Tax Office to the Commercial Registry Directorate, it was reported that during a tax audit conducted at "A" Limited Company it was determined that the company was not present at the address registered in the Commercial Registry. Consequently, the Commercial Registry Office notified the company and its partner "Y" that, pursuant to Article 33 of the Turkish Commercial Code (TCC), the change of address must be registered within 30 days. The company's partners determined the new registered office address as "P……." within the same neighbourhood via a general meeting resolution and had it registered with the Commercial Registry.

354. Associations and foundations are subject to structured registration and reporting through the DERBIS and VBYS systems respectively, which capture governance, financial and operational information and are directly accessible to competent authorities, supporting effective monitoring and transparency (See 5.3 and 5.5). Co-operatives are registered in the Trade Registry and recorded in MERSIS and are also subject to monitoring through the KOOPBIS platform to a limited extent; and given that co-operatives are also captured within MERSIS, the same limitations related to the use and verification of MERSIS registry information apply.

355. **BO Registry:** The introduction of the BO Registry in 2021 represents a significant enhancement of Türkiye's preventive framework. Additionally, BO information must be reported to the TRA under Tax Procedure Law General Communiqué No. 529 through periodic and event-driven notifications, with penalties for non-compliance. The accuracy of reporting may also be tested through tax inspections, while MASAK supervises the implementation of preventive measures under the AML Law No. 5549. Compliance has improved steadily, reaching approximately 99% by early 2025, reflecting sustained outreach, guidance and enforcement by MASAK and the TRA. This framework has substantially increased transparency regarding ownership and control of legal persons. Effectiveness of the overall regime is constrained by the gaps in verification. (See 5.3)

356. **Bearer shares:** Türkiye has not prohibited the issuance of bearer shares, but they are only permitted in a restricted and registered dematerialized form. Since the last evaluation, the country has taken meaningful steps to address the anonymity risks associated with bearer shares through the amendments to the TCC and the subsequent Communiqué of April 2021, which established a mandatory registration regime with the Central Securities Depository (CSD). The regime represents a genuine

improvement as noted in Türkiye's 2022 Follow-Up report, removing the anonymity of bearer share ownership. The CSD maintains electronic records of bearer share holders and transfers, which are accessible to competent authorities and administrative sanctions apply for failures to comply with notification requirements. Notably, the suspension of all shareholder rights — including dividend entitlements and general assembly participation — pending CSD notification provides a useful deterrent against non-registration. As of November 2025, 3,336 companies registered (0.20% of total companies) a total of 734,243 bearer shares held by 12,741 shareholders. Since the amendments in 2021, 8 companies have been audited (two in 2022, one in 2023, two in 2024 and three in 2025). A single shareholder was fined 27,240 TL (1.552,68 EUR) in 2022 for failing to report ownership on time. Despite these improvements, the bearer share dematerialisation regime may present a residual vulnerability. While transfers are effected upon physical delivery, the exercise of shareholder rights is contingent on notification to the CSD. In the absence of further clarification from the authorities on how this interim period is monitored or mitigated in practice, this could give rise to a situation where ownership is not yet reflected in the system, creating a temporarily non-transparent ownership state that could be exploited for passive asset concealment, evasion techniques and proceeds placement.

357. **Notaries**: The role of notaries at key corporate events — including incorporation under Article 335, capital increases and amendments to articles of association under Articles 454 and 456 and share transfers in limited liability companies — does not provide sufficient AML/CFT safeguards against the misuse of legal persons. While notarial involvement ensures that the legal form of the transaction is properly executed and that the identity of the persons appearing before them is authenticated, their function does not extend beyond this. Notaries are not required to verify registered office addresses against physical evidence, to identify whether a director or shareholder is acting as a nominee for an undisclosed principal, or to inquire into the source of funds injected as capital. The result is a framework that provides formal legal authentication at key moments in a company's lifecycle without any substantive AML/CFT mitigation of the risk.

358. **Nominee Directors and Shareholders**: Türkiye has also taken targeted measures to address specific higher-risk features. Nominee directors and shareholders are not recognised under Turkish law, limiting anonymity. Nominee arrangements have not been identified as a key risk in the LPRA, and this is not reflected as an identified risk in the complex ML cases presented. However, competent authorities do not actively identify de facto nominee arrangements in practice through testing of the registry, despite the continued advertisement of such services, including nominee arrangements, by obliged entities.

359. **Dissolution of Inactive Companies**: Türkiye applies measures to address inactive companies, demonstrating sustained efforts to ensure compliance with reporting and transparency obligations; however, some limitations remain in addressing repeated misuse of legal persons. The TRA as an ongoing programme of monitoring inactive companies and actively strikes off inactive companies, with 38,306 entities struck off in 2021, 38,021 in 2022, 40,534 in 2023, 44,105 in 2024, and 26,960 in 2025, reflecting continuous action to mitigate the risk of dormant companies. The dissolution of inactive companies provides a meaningful structural control. However, there is limited information on whether complementary measures target the individuals behind these entities, including whether directors, shareholders or beneficial owners associated with struck-off companies are monitored, restricted or sanctioned in cases of repeated involvement. In the absence of such measures, particularly given the repeated use of shell and front companies identified in typologies, these actions address the legal entity risk to a certain extent but not the underlying risk, which may persist through the continued activity of the same individuals.

360. **Financial Transparency Measures**: Financial transparency measures in Türkiye contribute to transparency to a limited extent for commercial legal persons and to a better extent for associations and foundations. For joint stock and limited liability companies, financial statements must be prepared and submitted to the tax authorities; companies subject to independent audit—determined by size thresholds or sector—are additionally required to make financial information publicly available (e.g. via a company

website), and listed companies must publish their financial statements on the Public Disclosure Platform (KAP). General and limited partnerships are similarly required to keep accounts and meet tax reporting obligations, but are not subject to public financial disclosure requirements. Ordinary partnerships do have obligations but do not have legal personality; while they may maintain accounts for operational purposes, tax obligations, as is typically the case, are borne at the level of the partners, who are required to declare income individually. Co-operatives are also required to maintain accounting records and comply with applicable reporting obligations, with relevant information recorded in systems such as MERSIS and subject to monitoring through KOOPBIS. When considered in light of the risk context identified in the LPRA—particularly the higher risks associated with capital companies—and the limited use of enforcement measures for fraudulent activities, these financial transparency measures appear to contribute only to a limited extent to the detection and prevention of misuse of legal persons in practice. By contrast, associations and foundations are required to submit financial and operational information through dedicated systems (DERBIS and VBYS), which are accessible to competent authorities and support ongoing monitoring, contributing to financial transparency and oversight to a better extent for other legal persons.

361. **Foreign Created Legal Persons with sufficient links**: Foreign-created legal persons with sufficient links are subject to the same BO reporting obligations as other corporate taxpayers. In addition to BO filing requirements, preventive measures applicable to legal persons—including those related to registration, CDD and monitoring—apply where relevant. In practice, the effectiveness of these measures is primarily evidenced through enforcement actions related to BO reporting obligations, particularly in relation to limited taxpayers. Overall, effectiveness for foreign-created legal persons remains constrained by the gaps outlined in Sections 5.2, 5.3 and 5.5, including limited enforcement in higher-risk areas such as MERSIS-related obligations and fraudulent companies, which is not fully aligned with the risk profile and is consistent with the more limited understanding of risks related to foreign-created legal persons (see 5.1).

5.3. Legal persons: Timely access to adequate, accurate and current basic and beneficial ownership information

Multi-pronged approach of Türkiye

362. Türkiye's multi-pronged approach to obtaining BO information, draws on several complementary sources. These include the BO Registry maintained by the TRA based on tax declarations, information collected by obliged entities through CDD measures, MoT records such as the Trade Registry Gazette and MERSIS database, and the CSD for dematerialised bearer shares. This framework is supported by cross-checking mechanisms, including controls conducted through MASAK's databases and audit processes.

Basic Information – Adequate, Accurate, and Up to Date

363. Türkiye collects and maintains basic information on domestic and foreign created legal persons with sufficient link to Türkiye through the Trade Registry Gazette, MERSIS, DERBIS, VBYS and KOOPBIS (commercial companies, associations, foundations and co-operatives[28]). These systems provide structured basic information on all legal persons in Türkiye and foreign created legal persons (excepting limited taxpayers) with sufficient links. For commercial companies, at incorporation, all companies are required to submit information on shareholders, partners and directors, which is recorded in the Trade Registry and maintained through the MERSIS system. Registration and subsequent amendments are conducted electronically and reviewed by Trade Registry officials, with supporting documentation submitted through notaries before approval. However, no information was provided on how the accuracy of this information is substantively verified within MERSIS beyond formal checks, which focus on the completeness and

[28] Co-operatives are registered in the Trade Registry and recorded in MERSIS, consistent with other commercial companies, and are also subject to monitoring through the dedicated KOOPBIS platform, which is used by co-operative managers and trade directorates.

consistency of submitted documentation, and compliance with procedural and legal requirements. The registry data is also not used for more analytical or risk-based verification, such as identifying multiple entities registered at the same address, mapping common directors or shareholders across companies, detecting complex or rapidly changing ownership structures. In practice, notaries appear to perform primarily formal compliance functions—ensuring that documents are complete and correctly executed—rather than verifying the underlying accuracy or truthfulness of the information submitted. Similarly, lawyers do not have a formal role in verifying the accuracy of ownership information in registry systems and, where involved, their role is generally limited to drafting articles of association, preparing documentation and filing-related activities, rather than acting as an independent validation mechanism. While the system provides transparency and traceability through public access to Trade Registry Gazette and MERSIS records, there is no systemic or systematic verification of information contained in the registry.

364. For other legal persons, more structured monitoring and compliance mechanisms are in place. Associations and foundations are subject to registration and reporting requirements, with information recorded in the DERBIS and VBYS systems respectively. These systems include broader datasets (e.g. governance, financial and asset-related information) and are directly accessible to law enforcement authorities. Robust risk-based monitoring and administrative and proportionate and dissuasive sanctions, ensure to a good extent compliance and data quality (See 5.5, IO.10 and R.8).

Beneficial Ownership Information - Adequate, Accurate, and Up to Date

365. Türkiye has adopted a definition of BO that is aligned with the FATF standard, focusing on the identification of the natural person(s) who ultimately own or control a legal person, whether through direct or indirect ownership, control through other means, or, where no such person can be identified, senior managing officials as a last resort (See R. 24). The BO Registry contains structured information on beneficial ownership and control, including for foreign legal persons. MASAK, the TRA, TIB have direct access to the BO Registry and other competent authorities including law enforcement can access the information upon request to MASAK or the TRA. Co-ordination between MASAK and the TRA and the integration of BO reporting into routine tax processes along with penalties for non-compliance have contributed to high compliance with BO filing obligations (See 5.5).

366. Verification of basic and BO information is conducted through targeted cross-checks, inspections, and discrepancy analysis, including comparison exercises between the BO Registry and the Trade Registry. These measures have identified inconsistencies and led to corrective actions and sanctions, demonstrating that verification, to some extent, occurs in practice. However, verification remains largely ad hoc and is not organised under a comprehensive, planned, risk-based framework covering all registries holding ownership information. Following the establishment of a WG in 2021 and the signing of co-operation protocols in June/July 2021, a joint data-matching project was initiated in 2022 comparing MoT and TRA records, identifying 240 violations out of 355 taxpayers. The project was re-initiated in March 2024, identifying 120 violations out of 188 taxpayers, with fines imposed and the BO Registry updated. In parallel, tax inspections identified 89 taxpayers with incorrect BO information. These exercises are valuable efforts towards ensuring baseline verification. But their effectiveness is limited without more sophisticated checks especially for higher-risk legal persons, complex structures and foreign-created legal persons with sufficient links. The authorities also indicated that in 2025, the TIB examined 66 656 taxpayers and verified BO Registry information for each taxpayer subject to reporting requirements. While the verification of BO for 66 656 taxpayers demonstrate a significant level of activity, limited information was provided on the methodology, scope and depth of these checks, how they connect to other discrepancy detection mechanisms, or whether they apply to foreign-created legal persons with sufficient links to Türkiye. Based on the information available, these checks include elements of identity verification of beneficial owners; even where this is limited to confirming that an individual is who they claim to be, it represents a meaningful step in establishing a basic level of accuracy. However, identity verification alone does not address whether the identified individual is in fact the true beneficial owner. There is limited evidence of meaningful checks to

verify the basis on which a person is identified as a beneficial owner, including whether they genuinely exercise ownership or control. As such, while these efforts, to some extent, provide an important initial safeguard, their effectiveness is constrained by the ad hoc nature of the checks, the quality of verification and the absence of a systematic, risk-based approach to verification.

367. FIs and DNFBPs in Türkiye are subject to CDD obligations under the AML/CFT framework, which require them to identify and verify the identity of their customers, determine and take reasonable measures to identify the BO, and understand the ownership and control structure of legal persons when establishing a business relationship or conducting transactions above the applicable thresholds. These obligations also include ongoing monitoring of the business relationship, keeping information up to date, and applying enhanced due diligence measures in higher-risk situations. FIs and DNFBPs use MERSIS to some extent and the BO registry to a lesser extent to supplement their CDD processes. FIs and DNFPBs obtain BO information primarily through their own CDD processes, including customer declarations and supporting documentation. Because of tax confidentiality provisions, Turkish authorities provide FIs and DNFBPs with an indirect means of accessing information in the BO Registry, whereby they may request from customers an official document containing BO data with a QR code, the authenticity of which can be verified. While FIs and DNFBPs can indirectly access the BO Registry though a customer-provided QR code, the number of taxpayers generating QR codes for sharing information with obliged entities and DNFBPs remains relatively low, with 21 721 in 2022, 68 406 in 2023, 71 774 in 2024 and 38 700 in 2025 (**Table 5.2 refers**).

368. When considered against the total population of approximately 1.6 million companies and a significantly larger number of potential beneficial owners, these figures suggest that the mechanism is not widely used in practice. This is further reflected in BO discrepancy related STR) data, where reports linked to BO verification through QR-coded documents total 2 490 between 2022 and 2025 and are overwhelmingly submitted by banks, with limited engagement from other FIs and no evidence of reporting by DNFBPs (**Table 5.3 refers**). However, no information was provided that demonstrates how competent authorities act upon such reports in practice. In particular, it remains unclear, in practice, whether authorities request corrections or updates to BO information, whether obliged entities in line with a risk-based approach have taken appropriate mitigating measures (such as restricting or closing accounts or business relationships), or whether such discrepancy reporting results in automatic or targeted sanctions, including administrative fines. While the reporting of BO discrepancies by obliged entities is a positive feature of the framework, the absence of information on specific follow-up actions, remedial measures or outcomes significantly limits the overall value of this process in improving the accuracy and reliability of BO information in practice.

Table 5.2. Statistics on the number of Official Documents issued through Interactive Tax Office[29]

Year of Inquiry	Number of Documents	Number of Taxpayers Creating Documents (Unique Tax ID)
2022	26 690	21 721
2023	87 626	68 406
2024	93 973	71 774
2025*	45 890	38 700
TOTAL	**254 179**	**200 601**

[29] This mechanism (QR coded documents) was established in 2022 therefore 2021 statistics are not available.

Table 5.3. STRs on beneficial ownership resulted from TRA's QR coded documents

Sector	2022*	2023	2024	2025	TOTAL
Banks	392	954	659	263	2 268
Factoring	2	1	21	0	24
Financing	1	3	3	1	8
Leasing	1	0	2	0	3
EO	0	0	0	9	9
CASPs	0	4	0	3	7
PEMIs	22	65	56	23	166
Capital Market Intermediary	2	1	0	2	5
TOTAL	**420**	**1 028**	**741**	**301**	**2 490**

* This mechanism (QR coded documents) was established in 2022 therefore 2021 statistics are not available

Availability to Competent Authorities

369. BO information must be provided to competent authorities upon request. There are explicit requirements in law to ensure that BO information is accessible within specific timeframes. Selected case examples shared by MASAK demonstrate that BO and related company information can be accessed and transmitted within relatively short timeframes, typically within a few days to around one week, with some larger or more complex requests taking several weeks. This is representative of the close working relationship seen between MASAK and LEAs. These examples involve requests from Chief PPOs and LEAs authorities between 2023 and 2025 and include ownership, partnership, management and BO records. While these cases illustrate good timeliness in practice, they do not indicate whether the information provided was complete and accurate at the time of transmission, whether follow-up requests were required, or whether any delays arose due to incomplete, inaccurate or unavailable information. In addition, the use of such information appears to be primarily driven by LEAs, with no recorded cases of supervisors making such requests, and no information on the frequency of access requests, or instances where access was delayed. No specific information was provided on access to adequate, accurate and up-to-date information on foreign-created legal persons with sufficient links to Türkiye, or whether timelines differ in such cases.

370. LEAs primarily rely on MASAK for information as no instances of requests to FIs, DNFPBs or companies for information on domestic legal persons or foreign created legal persons with sufficient links were evidenced. While Türkiye has a well-developed multi-prong framework, its effectiveness is constrained by a concentration of reliance on the BO Registry. In practice, authorities appear to rely significantly on MASAK as a central node, with information flows largely dependent on data derived from the BO Registry, creating a degree of circularity in the use of BO information. There is limited evidence that competent authorities seek or use BO information directly from FIs, VASPs, DNFBPs, or legal persons themselves. Although obliged entities are required to report discrepancies and penalties are imposed for non-compliance with CDD obligations, no information was provided on how discrepancy reports are used. The different elements of the multi-pronged framework operate largely in parallel, reducing the extent to which the benefits of the multi-pronged system are fully leveraged to improve data accuracy or mitigate risks from legal persons.

371. Türkiye's public procurement framework does not clearly provide public authorities with the powers to obtain timely access to BO information in the course of public procurement. While the Public Procurement Law and associated regulations establish a framework for verifying the legal identity of bidders, authorised representation, and certain registry-based ownership information through systems such as EKAP (Electronic Public Procurement Platform), these controls primarily rely on data from sources such as MERSİS and focus on legal ownership and representation, and therefore the deficiencies within

MERSIS apply to this aspect of the public procurement process and representation. There is no clear requirement for contracting authorities to access BO information, including from a BO Registry, nor for bidders or contract recipients to provide such information as part of procurement processes. In this context, although the framework supports transparency and traceability of procurement procedures, it does not ensure access to BO information as a component of risk mitigation, which is relevant given Türkiye's identification of corruption as a medium risk in its NRA.

372. In the context of international co-operation, Türkiye's competent authorities, including MASAK and Public Prosecutors, have demonstrated their ability to respond to requests for BO information, including through mutual legal assistance and other forms of co-operation. No concerns have been raised by international partners regarding the accuracy or reliability of the information provided. BO information is obtained through a multi-pronged framework, drawing on registries as well as information held by FIs and DNFBPs, with MASAK able to request such information from relevant entities in support of foreign requests. Access to BO information held in registries appears to be relatively timely, and information is generally provided without delay, with any delays in mutual legal assistance primarily arising in more complex cases requiring additional investigative measures. However, no information was provided on access timelines through other mechanisms beyond registries.

5.4. Legal arrangements: Timely access to adequate, accurate and current basic and beneficial ownership information[30]

373. Türkiye's legal framework does not recognise trusts or equivalent domestic legal arrangements. Authorities have substantiated this position through legal analysis and empirical checks of registries, tax records and supervisory information, and this conclusion is appropriately reflected in the LPRA.

374. Mechanisms exist to obtain information on foreign legal arrangements that have a nexus with Türkiye, including arrangements owning domestic assets or maintaining financial accounts. Competent authorities have legal powers to request relevant information from FIs and DNFBPs where such relationships are identified.

375. FIs demonstrate awareness of their obligations to identify and report relationships involving foreign legal arrangements, supported by written guidance and requirements imposed by supervisors. These mechanisms provide a basis for accessing information when such risks arise.

376. Competent authorities in Türkiye have legal powers to request relevant information from FIs and DNFBPs where such relationships are identified. In practice, this provides an important channel for accessing information on legal arrangements, particularly where these are part of customer relationships subject to CDD and BO requirements. Through MASAK's powers and supervisory frameworks, authorities are generally able to obtain available information in a timely manner when such arrangements are visible within the regulated sector.

377. However, the effectiveness of this mechanism is constrained by Türkiye's overall gaps in understanding of legal arrangements. As the NRA does not identify trusts or similar legal arrangements as a significant domestic feature, there is limited direct focus on these structures. This more limited understanding affects the extent to which legal arrangements—particularly those established abroad—are consistently identified within ownership structures, thereby limiting the capacity to identify potential beneficial ownership risks, hidden control relationships, and complex ownership chains. As a result, while mechanisms exist to obtain information, their practical effectiveness depends on whether such

[30] See the Methodology for Recommendation 25 regarding beneficial ownership information for legal arrangements.

arrangements are first recognised and captured within the system, which may impact the completeness and timeliness of information obtained in practice.

378. In practice, no cases involving foreign trusts or similar arrangements were identified during the reporting period. While this reflects a low assessed risk, it also means that information-gathering powers may not have been tested extensively in operational cases. As a result, assurance that emerging risks related to foreign legal arrangements would be identified and addressed in a timely and systematic manner remains limited.

5.5. Effectiveness, proportionality and dissuasiveness of sanctions

379. Türkiye has strengthened its sanctions framework for breaches related to the transparency of legal persons and BO, with evidence of active enforcement; however, certain elements of the regime remain limited in their overall dissuasiveness. Administrative sanctions—particularly those linked to BO obligations—have been significantly increased and consistent application has contributed to high levels of compliance, including near-complete BO filing rates. Authorities also apply sanctions to associations and foundations, which appear broadly aligned with the risks identified in the non-profit sector, and make active use of measures to strike off inactive companies, although the absence of safeguards preventing the same individuals from establishing new legal persons limits the effectiveness of this tool. Türkiye has dematerialized bearer shares, enhancing transparency, although penalties for related breaches remain modest and unchanged from the 2022 follow-up report. Some important tools—such as the dissolution of companies under Article 210/3 of the TCC—are used only sparingly. Sanctioning in relation to MERSIS registry obligations remains particularly limited, and, combined with the absence of criminal liability for legal persons - (see Chapters 7 and 9: IOs 7 and 9), the framework relies predominantly on administrative fines which may not be sufficiently dissuasive, particularly for larger or more complex legal persons.

380. Sanctions for breaches of BO obligations have been significantly strengthened and are actively enforced in practice. Under Article 355/bis of the Tax Procedure Law, administrative fines are adjusted annually and, as of 2025, violations trigger an automatic tripling of the base fine to TRY 84 000 (EUR 2 304), with an additional 25% increase for repeat offences within two years. These measures are applied through inspections and administrative actions, with fines reaching TRY 291 M (EUR11.9 M) across 49 171 taxpayers in 2023 and TRY 258 M (EUR 7.2 M) across 14 764 taxpayers in 2024. The use of enhanced penalties for repeat violations—totalling TRY 180 M (EUR 7.38 M) in 2023 and TRY 231 million (EUR6.48 M) in 2024—demonstrates a functioning corrective mechanism, contributing to high levels of compliance (99.02%) with BO reporting obligations. This represents a useful tool to ensure compliance with a newer reporting mechanism; as a next step, its application could be further leveraged to support the accuracy and timeliness of BO information.

381. Administrative fines against foreign-created legal persons for failure to comply with BO reporting obligations demonstrate effectiveness to some extent in promoting compliance but are limited as they do not address the accuracy of information. The sanctions imposed apply only to limited taxpayers (foreign-created legal persons with a taxable presence), with 55 entities sanctioned between 2021 and 2025, resulting in fines of approximately TRY 432 900 (EUR 12 806), and an additional TRY 294 000 (EUR 7 431) for repeated violations in 2024–2025. This represents the only evidence of enforcement action against foreign-created legal persons with sufficient links, with no information provided on measures applied to other foreign-linked entities, including those with more than 50% foreign shareholding, indicating a narrow and incomplete enforcement approach relative to identified risks.

382. In parallel, Article 15 of the AML Law provides for imprisonment (six months to one year) or judicial fines for undisclosed front person activity, with enforcement increasing from 909 investigations and 143 convictions in 2021 to 1 262 investigations and 689 convictions in 2024 (893/654 in 2025). Conversion rates

for front person activity have improved significantly, with investigation-to-conviction rates increasing from approximately 16% in 2021 to 55% in 2024 (73% in 2025), and prosecution-to-conviction rates rising from 16% to 78% (81% in 2025), demonstrating more effective case progression and judicial follow-through. While this demonstrates active use of the provision and partial effectiveness, information was unavailable on the nature and complexity of cases, the application of custodial versus financial sanctions in practice, their relevance to higher-risk ML/TF scenarios, and if there are measures in place to address persistent non-compliance.

383. Sanctions imposed by the MoT under the TCC are the least developed element of the framework, particularly given the higher-risk exposure identified in the LPRA for commonly used corporate forms and sectors vulnerable to misuse. Enforcement under Articles 33/2, 38/1, 64, 65, and 562/13(a)—covering registration, trade name accuracy, and bookkeeping obligations—has been relatively limited in practice, with only a small number of companies sanctioned annually (generally between 3 and 10 cases) and modest fines, demonstrating that enforcement activity is not fully aligned with the identified risk profile (**Table 5.6 refers**). Several provisions show limited consistency in enforcement, suggesting that more systematic verification of core registry information, including address data, could be beneficial. While LEAs have indicated that identifying multiple or suspicious addresses is a key starting point in detecting misuse, this type of basic verification could be more proactively undertaken at the registry level. In parallel, although Article 210/3 of the TCC provides for the dissolution of companies engaged in fraudulent or unlawful activities, it has been used only in a small number of cases (4 in 2021, 2 in 2022, 4 in 2023, 3 in 2024, and 5 in 2025). Strengthening the use of these tools—particularly at the stage of ongoing operations—could further enhance the reliability of corporate information and help mitigate risks related to the misuse of legal persons, including for concealing beneficial ownership and ML/TF related financial flows.

384. Sanctions applied through DERBIS (for associations) and VBYS (for foundations) indicate active enforcement of compliance obligations in the non-profit sector, primarily targeting failures in reporting, registration, governance, and transparency requirements. Under DERBIS, sanctions relate to breaches such as non-compliance with notification and reporting obligations, with 444 associations sanctioned in 2021, 339 in 2022, 348 in 2023, 218 in 2024, and 281 in 2025 (as of November), and total penalties reaching TRY 17.3 M (EUR 379 818) in 2025 (**Table 5.5 refers**). Under VBYS, sanctions on foundations—primarily for violations including non-submission of annual declarations, deficiencies in internal audit reports, failures to declare foreign donations, and non-compliance with notification obligations (e.g. management changes, address updates, and real estate declarations)—increased from TRY 1.9 million (EUR 109 165) in 2022 to TRY 10.7 million (EUR 235 275) in 2025 (**Table 5.4 refers**). These sanctions form one element of robust ongoing monitoring efforts by authorities to ensure that information is accurate, and up to date and the sanctions applied to associations and foundations are effective, proportionate, and dissuasive.

385. Türkiye has not prohibited the issuance of bearer shares of companies not listed on a stock exchange, but since 2022 has dematerialized the issuance of bearer shares, enhancing transparency and reducing risks associated with anonymous ownership (See R.24). Nevertheless, penalties for breaches of bearer share requirements remain modest, with a single penalty applied, indicating that while transparency has improved, and the sanctions framework has not been further strengthened and is not dissuasive. (See 5.2 above).

Table 5.4. Sanctions imposed by VBYS on Foundations (2022-2025)*

Name of the Transaction Subject to Administrative Fine	Number of administrative fines imposed				Administrative fine amount (EUR)			
	2022	2023	2024	2025**	2022	2023	2024	2025
Branch/Representative Office Opening	0	9	2	4	0.00	1,937.99	466.03	973.57
Branch/Representative Office Closure	1	1	1	2	134.29	215.33	147.06	526.99
Annual Declaration	116	213	153	240	14,964.32	44,533.95	32,563.72	59,130.57
Receiving Aid/Donations from Abroad	106	98	42	87	12,030.31	20,431.86	8,902.21	22,132.75
Donating/Aiding Abroad	74	11	8	29	8,260.55	2,368.65	1,864.13	6,947.20
Real Estate Declaration	169	129	112	106	19,860.85	27,421.62	25,582.03	25,054.96
Establishing an Economic Enterprise/Company	30	14	26	15	3,693.83	3,014.65	6,058.42	3,563.23
Closure of Economic Enterprise/Company	13	9	12	20	1,666.22	1,937.99	2,796.19	4,787.42
Internal Audit Report	187	181	275	342	23,811.64	36,115.83	51,528.54	72,272.73
Account Statement of Mülhak Foundations	3	12	8	5	295.83	1,820.24	1,434.33	928.29
Change of Address and Contact Information	19	7	10	23	2,375.76	1,388.59	2,244.20	4,778.27
Foundation Management Change	166	146	133	132	20,737.34	30,081.04	29,534.68	32,678.32
Other	11	6	28	6	1,334.48	1,173.26	6,266.57	1,500.55
Total number of administrative fines imposed.	895	836	810	1011	109,165.42	172,441.00	169,388.11	235,274.85
Number of Foundations That Received Administrative Fines	535	536	534	684				

Note: (*) Data for 2020 and 2021 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025); (***) Conversion rates were calculated on annual average bases as follows: year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); and year 2024 (1 TRY= 0.028).

Table 5.5. Sanctions imposed by DERBIS on Associations

Period	Administrative Fine	Judicial Action	Judicial Action and Administrative Fine	Total Fine	Total Administrative Penalties Imposed (TRY)	Total Administrative Penalties Imposed (EUR)***	Total Administrative Penalties Imposed (US)
2021	370	21	53	444	1,665,365	161,540.41	124,532.00
2022	273	23	43	339	4,724,000	269,268.00	251,812.00
2023	301	18	29	348	12,708,342	521,042.02	430,354.00
2024	189	11	18	218	4,196,985	117,515.58	118,559.00
2025*	243	9	29	281	17.638.703,62	388.051,48	415.126.00

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025). (***) Conversion rates were calculated on annual average bases as follows: year 2020 (1 TRY=0.12 EUR); year 2021 (1 TRY= 0.097 EUR); year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); year 2024 (1 TRY= 0.028); and year 2025 (1 TRY= 0.022 EUR).

Table 5.6. Sanctions imposed by MERSIS on companies (2021-2025)

	TCC Articles				
	33/2	38/1	64	65	562/13a
2021			6,190.00 ₺ (600,43EUR) (3 companies)	108,387.00₺ (10.513,54 EUR) (4 companies)	
2022			314,944.00 ₺ (17.951,81 EUR) (7 companies)		27,240.00₺ (1.552,68 EUR) (1 shareholder)
2023			163,036.00 ₺ (6.684,48 EUR) (4 companies)	222,031.00₺ (9.103,27 EUR) (4 companies)	
2024			884,553.00 ₺ (24.767,48 EUR) (10 companies)	147,822.00₺ (4.139,02 EUR) (1 company)	
2025		41,796.00 ₺ (919,51 EUR) (1 company)	479,061.00 ₺ (10.539,34 EUR) (5 companies)	344,918.00₺ (7.588,20 EUR) (3 companies)	

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025); (***) Conversion rates were calculated on annual average bases as follows: year 2020 (1 TRY=0.12 EUR); year 2021 (1 TRY= 0.097 EUR); year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); year 2024 (1 TRY= 0.028); and year 2025 (1 TRY= 0.022 EUR).

386. Sanctions for BO violations under Article 17/A of the RoM demonstrate that Türkiye applies administrative measures for non-compliance, particularly across FIs, including banks and PEMIs, where most observed violations are concentrated (**Table 5.7 refer**s). MASAK has implemented some remedial actions and has imposed fines for non-compliance with CDD measures to some extent but an overall positive impact from such measures has yet to be demonstrated. In addition, the legal design of the sanctioning regime—where fines are largely imposed on a per breach basis through fixed statutory amounts, with transaction-based minimum thresholds applying only to certain financial institutions and not DNFPBs—limits the extent to which penalties can reflect the overall seriousness or scale of breaches. As a result, while sanctions are being applied, they are not proportionate to the nature and scale of violations and are not sufficiently dissuasive in practice, particularly in higher-risk sectors.

Table 5.7. BO Violations in AML/CFT Supervisions by Obliged Entities

Year	Sector	Number of Obliged Parties in violation	Number of Violations	Administrative Fines (TRY)	Administrative Fines (EUR)
2020	Banks	1	6	214 360	25 723
	PEMIs	3	13	167 080	20 050
	Factoring Companies	1	2	66 928	8 031
	Leasing Companies	1	3	90 210	10 825
TOTAL		**6**	**24**	**538 578**	**64 629**
2021	PEMIs	3	23	386 533	37 494
	Factoring Companies	1	3	90 210	8 750
	Crypto Asset Service Providers	4	15	450 000	43 650
TOTAL		**8**	**41**	**926 743**	**89 894**

2022	Banks	5	35	2 100 000	119 700
	PEMIs	2	13	862 472	49 161
	Factoring Companies	3	13	866 880	49 412
	Financing Companies	1	1	81 720	4 658
	Leasing Companies	1	8	1 763 502	100 520
TOTAL		**12**	**70**	**5 674 574**	**323 451**
2023	Banks	1	5	609 516	24 990
	PEMIs	2	18	1 820 808	74 653
	REAs	7	20	611 217	25 060
	DPMS	3	7	220 149	9 026
	Vehicle Traders	2	5	254529	10 436
	VASP	1	1	91 089	3 735
	Lawyers	1	3	273 267	11 204
	Accountants	6	17	1 247 139	51 133
TOTAL		**23**	**76**	**5 127 714**	**210 236**
2024	DPMS	1	1	99 386	2 783
	EOs	1	1	198 772	5 566
	Accountants	3	6	596 316	16 697
TOTAL		**5**	**8**	**894 474**	**25 045**

6 Financial intelligence

The relevant Immediate Outcomes considered and assessed in this chapter is IO.6. The Recommendations relevant for the assessment of effectiveness under this chapter are R.29-32 and elements of R.1, 2, 4, 8, 9, 15, 34, and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Türkiye's Financial Intelligence Unit (FIU), MASAK, is an administrative-style FIU and serves as the central authority for receiving, analysing, and disseminating STRs. MASAK's direct access to more than 300 databases, cross-border declarations, and disclosures, combined with STR data, provides a robust information base that enables the production of high-quality quantitative and qualitative financial intelligence and underpins its role as the main authority to produce financial intelligence. Other competent authorities access financial and non-financial information through their own databases and can obtain additional data from MASAK, where needed, to support investigations and intelligence.

b) Between 2020-2025, MASAK received approximately 2.7 M STRs from FIs, DNFBPs and, since 2023, from VASPs. Most STRs were reported from high-risk sectors in line with Türkiye's 2023 and 2025 NRAs findings (including 63% from the banking sector, 26% from PEMIs, and 7% from VASPs which have been recently regulated). However, several DNFBPs sectors consistently file low numbers of STRs even when considered as medium risk in the respective STRs (i.e., public accountants reported less than 1% STRs).

c) The majority of submitted STRs are related to high-risk and medium-risk predicate offences, such as, illegal betting and gambling (32%), tax evasion (24%), and fraud (13%) which to some extent is commensurate with the country risk profile. However, the number of STRs related to other predicate offences also categorised as high or medium risks remains very low (TF, drug trafficking, customs smuggling and human/migrant smuggling) indicating reporting entities have challenges in identifying the underlying predicate offence behind the transaction being reported.

d) MASAK analysed 1.2 million STRs (46%) mostly as part of their strategic analysis work, which is significantly higher than those that are mandatory to review during the scoring process which only represents the 8% of the total submitted STRs. However, only 16% of these STRs are used for ML, TF, and predicate offences operational analysis and examination. 76.4% of MASAK's analysis work is dedicated to TF files, which is aligned with the country's risk profile given Türkiye's exposure to terrorism and TF threats.

e) Türkiye has a robust system that allows MASAK to produce good quality financial intelligence and all other relevant information to appropriately support operational needs when conducting ML, associate predicate offences and TF investigation and prosecutions. MASAK proactively and reactively produces similar number of reports demonstrating a balanced approach and strong capability to produce financial intelligence. MASAK also identifies and traces complex ML/TF cases, including criminal networks using a combination of different channels to launder proceeds of crimes and finance terrorist activities which has been proven through different case studies.

f) Competent authorities make effective and systematic use of MASAK's financial intelligence, with its reports consistently assessed as high quality, relevant, and of clear added value to AML/CFT investigations, as demonstrated by multiple case studies. However, some delays in the production of these reports were identified, which were considered to slightly affect the timeliness of enforcement actions in certain cases. Competent authorities have demonstrated a consistent use of financial intelligence to pursue positive results in their ML, associate predicate offences and TF investigations

g) Türkiye has established solid formal and informal interagency co-operation mechanisms for operational purposes which have resulted in the effective use of financial intelligence and disruption strategies when investigating ML, associate predicate offences and TF.

Other Recommended Actions

a) Design and implement an operational strategy to increment the use of high score STRs with the aim of increasing spontaneous dissemination of financial intelligence reports.

b) Enhance and periodically review the use and quality of disseminated financial intelligence reports to better support the operational needs of public prosecutor and LEAs in line with Türkiye's ML/TF risks.

c) Improve the timeliness of responding to judicial requests other than TF cases, to timely respond to LEAs and judicial request on ML and associate predicate offences and ensure the effectiveness of financial and other information exchange between MASAK, LEAs, and judicial authority.

d) Continue developing the IT system to support MASAK's production financial intelligence both for operational and strategic analysis.

e) Raise awareness on TF indicators for reporting entities (FIs, DNFBPs and VASPs) prioritising those at a major risk of being abused.

Overall Conclusions on IO.6

Türkiye has a robust institutional and operational framework for the production and use of financial intelligence which has demonstrated to strongly support ML, associate predicate offences and TF investigations. MASAK plays a pivotal role in the AML/CFT/CPF system and is the main authority responsible for producing financial intelligence. To perform its duties, MASAK directly accesses 300 data bases and cross-border declaration and disclosures which coupled with the collection of all data from submitted STRs and financial analysis produced, creates a solid cross-verification system that contributes to the quality of the financial intelligence being disseminated. Other competent authorities also have access to a wide range of information through their data bases and can request MASAK to provide them with financial intelligence in the context of a criminal investigation.

STRs are one of the main sources of information used by MASAK when producing financial analysis. The number of STRs received (2.7 million) are generally in line with the country's risk profile as the majority are related to illegal betting and gambling (32%), tax evasion (24%), and fraud (13%). However, submissions related to other high or medium-high risk offences remains very limited, for example, TF (1%) and drug trafficking, customs smuggling and migrant/human smuggling (0%).

From the total STRs received, MASAK analysed 1.2 million STRs (46%) mostly as part of their strategic analysis work, which is significantly higher than those that are mandatory to review during the scoring process which only represents the 8% of the total submitted STRs. However, only 228.770 STRs (16%) were used for ML, TF, and predicate offences operational analysis and examination. In addition, 76.4% of MASAK's analysis and dissemination work is related to terrorism/TF cases in line with the country's risk profile.

Türkiye's competent authorities have close formal and informal co-operation mechanisms in place to exchange financial intelligence and other relevant information to pursue ML/TF investigations and prosecutions. Public prosecutors, LEAs (in particular, TNP and GGC) and MASAK have demonstrated to formally share information on daily basis through the UYAP system but also through case-specific strategy co-ordination round tables. Close ad hoc and formal interagency co-operation mechanisms between MASAK and competent authorities have proven to facilitate the exchange of financial intelligence leading to the disruption of large criminal networks and high-impact outcomes on investigations and the tracing of proceeds and instrumentalities. All competent authorities highlight the role, the quality and the timing of MASAK's financial analysis to pursue complex ML/TF/PF investigations including with transnational element, which was confirmed through case studies.

Türkiye is rated as having a Substantial level of effectiveness for IO.6.

Click or tap here to enter text.

Immediate Outcome 6

387. Since its 2019 MER, Türkiye has undertaken various initiatives to expand data access and improve the efficiency of financial intelligence analysis and production including as part of its ICRG action plan. Türkiye has transitioned all AML/CFT/CPF competent authorities data registration into two interconnected electronic systems (UYAP and e-government) which has facilitated financial data collection. This allows Türkiye to identify and trace a full spectrum of information to develop robust financial profiles to support ML, associate predicate offences and TF investigations and prosecutions. Türkiye's FIU (MASAK) and LEAs

resources were also strengthened (e.g. number of strategic analysis analysts in MASAK doubled and kept increasing since in line with needs).

6.1. Timely access to relevant, accurate and up-to-date information

6.1.1. By the FIU

388. MASAK, is the country central authority for the receipt, analysis and dissemination of STRs. As an administrative-style FIU, it plays a pivotal role in Türkiye's AML/CFT/CPF system and is the main authority responsible for producing financial intelligence at an institutional and operational level. Due to the robustness of its dataset, MASAK accesses timely and up-to-date broad range of financial and non-financial information to a very large extent. MASAK's access to multiple sources of information is a major strength as it enables extensive real-time cross-checking and verification of data, significantly enhancing accuracy and reliability of the information when producing financial intelligence.

389. To perform its functions MASAK uses one offline (intranet connection) and one online system (internet connection). MASAK accesses a data set composed by more than 300 databases from public entities (32 data bases) and private institutions, legal persons' basic information (through MERSIS system), STRs (2 740 332 between 2020-2025), cross-border declarations or disclosures on currency (over 162 000) and financial analysis reports. Türkiye's competent authorities have moved all their data collection to an electronic format (UYAP system) allowing MASAK to have a direct extensive and real time access to up-to-date information which has greatly contributed to insource accurate data collection and to produce well-informed financial analysis and intelligence reports. Through these data bases, MASAK can access personal, basic and BO information, cash declarations/disclosures, criminal records, tax and revenue information, information on personal income, prior related STRs, including information registered by obliged entities (FIs, DNFBPs and VASPS), information hosted by the land and property, vessels and vehicles registries.

390. STRs are the main source of information inputting MASAK's work. Between 2020-2025, MASAK received approximately 2.7 M STRs from FIs and DNFBPs, and more recently VASP (see IO.3), with most of them emanating from the banking sector (63%), payment service providers and electronic money institutions (26%) and VASPs (7%), all of them identified as high-risk sectors in Türkiye's 2023 and 2025 NRAs. However, less than 1% STRs from public accountants have been registered which is not commensurate with the country's risk profile. In terms of quality, most STRs contain sufficient and qualitative information depending on the reporting sector, with those submitted by FIs generally being the most comprehensive ones. When the STRs lack sufficient information, MASAK requests additional information from the reporting entities to support its analysis. The below table provides an overview of the STRs received since 2020.

Table 6.1. STRs reported by FIs, DNFBPs and VASP sector (2020-2025)

Sector	Net Risk profile*			2020	2021	2022	2023	2024	2025**	Total STRs/reporting period	Ratio/ reporting period
	ML	TF	PF								
Banking Institutions	H	H	M	182828	205793	314700	432499	349988	235358	1721166	63%
PEMIs Institutions	M/H	M/H	M	46840	284544	74513	102776	110949	101987	721609	26%
VASP (CASP)	H	H	M	N/A	2233	20569	48678	63603	53490	188573	7%
EOs	M/H	M/H	M/L	2660	4500	6188	9108	5726	4315	32497	1%
Those Who Operate in The Field of Lotteries And Betting	M/L	M		262	36	64	1755	17301	6366	25784	1%

Factoring companies	M	M/L		1893	2729	2154	2277	3686	3631	16370	1%
Financing companies	M/L		L	165	497	1571	1325	1793	1048	6399	0%
Capital Market Brokerage Houses	M	M	L	368	692	595	897	1215	1088	4855	0%
Cargo companies		M/L		359	666	740	641	736	345	3487	0%
Insurance, reinsurance and pension companies		L	M/L	361	404	496	529	747	674	3211	0%
DPMS	M/H	M/H		51	138	320	683	1097	2161	4450	0%
Intermediaries of Precious metals and stones (jewelers)	M/L	L	M/L	0	0	0	0	1392	717	2109	0%
Financing leasing companies	M/L	L	L	12	60	335	302	295	342	1346	0%
Dealers of Any Kind of Sea, Air and Land Transportation of vehicles including construction machines	M			54	52	60	42	43	15	266	0%
Savings finance companies	L			0	0	12	13	15	488	528	0%
Notaries	L		L	5	24	22	4	1	3	59	0%
REAs		M/H	L	0	9	2	19	1	6	37	0%
Lawyers	M/L	L		0	2	0	3	3	0	8	0%
Asset management companies	L			0	0	1	4	1	4	10	0%
Independent audit institutions	M/L			2	1	0	0	0	0	3	0%
Portfolio management companies	M/L	L		0	0	0	0	3	6	9	0%
Other***				1671	2615	2980	0	0	290	7556	0%
Total				237531	504995	425322	601555	558595	412334	2740332	100%

Note: (*) Risk profile: ratings based on Türkiye's 2025 NRA (H: high risk; M/H: medium-high risk; M: medium risk; M/L: medium-low risk; L: low risk); (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025); Other**: including 42 STRs from public accountants received between 1 August-28 November 2025.

391. The numbers of STRs received are generally in line with the NRA findings. However, several DNFBPs sectors consistently file low number of STRs even when considered medium risks in the respective NRAs (i.e., exchange offices and DPMS). This raises concerns about the understanding of ML/TF risks obligations within these sectors (see IO.4).

392. Reporting entities submit STRs electronically by filling out an online form, which requires the reporting entity to indicate the underlying associate predicate offence and if the suspicious activity is related to ML, TF or PF, among other relevant information. While submitting the STR, the reporting entity receives automated messages with best practices on how to fill in the information to guarantee and alerts in case some relevant information has not been submitted. This system guarantees comprehensiveness of the information being submitted.

393. As outlined in the table below, the majority of submitted STRs are related to ML and associate predicate offences (99%) including, illegal betting and gambling (32%), tax evasion (24%), and fraud (13%) in line to some extent with the country's risk profile. However, the number of STRs related to some high-risk or medium high-risk predicate offences remains very low. For instance, between 2020 and 2025, MASAK received only 7961 STRs (0.3%) related to drug trafficking, 13699 on customs smuggling (0.5%) and 5 749 on migrant/human smuggling (0.2%). The low numbers of STRs received against predicate

offences categorised as high or medium-high risks indicates reporting entities have challenges in identifying the underlying predicate offence behind the transaction being reported.

394. In addition, TF STRs submissions remain very limited (1%) given Türkiye's risk profile, particularly across TF high-risk sectors likes banks (10 697 STRs), VASP (1 896 STRs), exchange offices (87 STRs), and payment and e-money institutions (4 747 STRs). Competent authorities explained that the reason behind the low number of submissions on of TF STR corresponds a lesser understanding of TF risk, except for targeted financial obligations, identification of suspicious more generally and complexity of establishing clear links between the transaction being reported (as a silo transaction) and terrorism/TF activity (see IO.3). For this reason, reporting entities revert to submit these STRs under a ML or an associated predicate offence. To overcome this challenge, MASAK implemented a scoring system which allows analysts to reassess the submitted information by cross-checking the information with previous submitted STRs and ongoing analysis on the TF Evaluation and Analysis departments, screening on all the names against the designations lists which allows MASAK to understand- at an early stage of the analysis process- if the isolated reported transaction corresponds to a TF scheme. MASAK identified all TF STRs as high priority.

Table 6.2. Breakdown of STRs by possible underlying offence (2020-2025)

Suspected offence	Risk Profile*	2020	2021	2022	2023	2024	2025**	Total/ offence	% of Total
Predicate offences									
Facilitating illegal betting and gambling	M/H	78919	311917	112219	161442	144643	126130	935250	32%
Tax evasion and tax avoidance	M	62768	66543	131016	186992	152866	95782	695967	24%
Fraud	H	16212	20025	24613	78673	126263	122623	388409	13%
Not declaring transactions for someone else's account		8734	17161	36370	61367	62959	47041	233632	8%
Cybercrime		6416	2940	3453	15054	16001	7533	51397	2%
Unlicensed payment and electronic money services		1963	3904	6390	10459	13260	8331	44307	2%
Offences related to capital markets		973	1610	2538	3927	4476	3990	17514	1%
POS usury	M/L	1973	1381	1233	2266	5048	8566	20467	1%
Forgery of official/private documents	M	4719	2097	3113	3713	2678	1484	17804	1%
Banking offences		221	364	1400	2610	5850	7869	18304	1%
Others***		72436	88498	116829	105941	63984	22782	470470	16%
ML/predicate offence		**255334**	**516440**	**439174**	**632424**	**598028**	**452131**	**2893521**	**98%**
Terrorism/TF	**H**	**1987**	**2785**	**2934**	**4037**	**3825**	**3907**	**19475**	**1%**
TF**	**H**	**2217**	**2757**	**4164**	**8520**	**5956**	**3898**	**27512**	**1%**
PF	**M/L**	**0**	**0**	**0**	**0**	**38**	**129**	**167**	**0%**

Note: (*) Risk profile: ratings based on Türkiye's 2025 NRA (H: high risk; M/H: medium-high risk; M: medium risk; M/L: medium-low risk; L: low risk); (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).; (***) Others: includes the following predicate offences: Money and valuable document fraud/forgery (13165 STRs); Customs smuggling (13699 STRs); Drug trafficking (7961 STRs); Usury (5355 STRs); Violation of obligations (2508 STRs); Crimes against property (theft, robbery, etc.) 2721(STRs); Migrant smuggling and/or human trafficking (5749 STRs); Smuggling of precious metals and stones (3881 STRs); Illegal bill payment centre activities (3008 STRs); Pyramid selling systems (Ponzi) (1966 STRs); Corruption and offences involving public officials (2667 STRs); Threats/blackmail/force and kidnapping (1748 STRs); Illegal aid and fundraising and solicitation (5589 STRs); Insurance fraud/ policy forgery (1125 STRs); Encouraging or facilitating prostitution (1765 STRs); Misuse of civil society organisation (913 STRs); Fuel smuggling (1859 STRs); Violation of social security legislation (662 STRs); Unauthorised VASP (CASP) activity (929 STRs); Smuggling of cigarettes, alcohol, tobacco products (709 STRs); Smuggling of weapons and ammunition (620 STRs); Obscenity (539 STRs); Smuggling of historical artefacts and trade in cultural property (728 STRs); other predicate offences (390604 STRs); (****) the TF STRs number is higher than STRs received under reporting category because a STR received from a obliged entity may include more than one crime.

395. MASAK has carried out activities aimed at increasing the accuracy and quality of STR reporting through training, supervision and workshops, publishing guidelines, and continuously reviewing the automated system messaged to raise awareness on how to submit the STR information.

396. At the analysis phase, MASAK can access- directly and indirectly- additional information, both online and offline, (i.e., personal information, cash declarations/disclosures, criminal records, tax and revenue information, information on personal income, including BO information of legal persons, among others) to verify and complement the STRs information. MASAK can also access MERSIS (legal person's basic information). A new data base integrated financial intelligence system (EMIS) was implemented in May 2025, from which MASAK analysts can access different layers of information according to the duties they perform and can access and filter the financial information needed case by case. STRs can be cross-checked against the other 300 data bases that integrates MASAK's data set to conduct the financial analysis, including access to other public institutions data bases, such as the revenue administration data, which keep records regarding economic activities, wealth items, tax liabilities, census information and illegal activities. Furthermore, MASAK can request any public institution, reporting entities, natural and legal persons, and any other organisation to provide all kind of information, documents and related records. These organisations shall fully and accurately provide the information requested including the necessary passwords to access the information or make these records decipherable.

397. MASAK has direct access to cross-border declarations (incoming: 132 699 transactions/ outgoing: 24 071 transactions) and disclosures (incoming: 54 475 transactions/ outgoing: 98 571 transactions) and the information on the number of seizures conducted by Customs Enforcement. If needed, the customs officer can request the passenger information regarding the cash or payment instruments being transported and report to MASAK in case there is a failure in the declaration or disclosure (See IO.8). This information is consistently integrated into the MASAK's data base.

398. When deemed necessary, MASAK can request information from their counterparts whether through the Egmont Group and/or the bilateral MOUs signed with 66 other jurisdictions. This broadens the scope of the MASAK's information including foreign-based financial intelligence.

6.1.2. By other competent authorities

399. Competent authorities also have access to a broad range of financial and non-financial information through their own databases to support their intelligence and investigative functions. While these databases are generally less comprehensive than MASAK ones, competent authorities can request their counterparts and stakeholders any type of information in the context of an investigation, including financial information hosted on MASAK's data bases. STR cannot be accessed by other competent authorities other than MASAK, courts during trials and examiners while conducting supervisions.

400. Prosecutors and courts can request MASAK to provide information on STRs in the context of a criminal investigation. In line with confidentiality rules, MASAK will share this information as an intelligence product including an annex of the raw data supporting the report. MASAK products are disseminated via electronic document management systems such as KEP and BELGENET, or by post depending on their level of importance.

401. Competent authorities conduct specific procedures to ensure that the sources of information contain relevant, accurate and up to date data. Public prosecutors and LEAs are legally obliged to supply and usually supply, as gathered from interviews during the onsite visit, the knowledge and documents needed for an ongoing investigation without delay.

402. The GGC, the TNP and the Coast Guard Command (CGC), can also access a broad range of information to perform its functions. TNP and GGC have direct access other competent authorities' databases and information systems such as UYAP (National Judgement Network Project), KPS (Identity and Address Sharing System), DERBIS (Association Information System), VBYS (Foundation Information Management System). Among other law enforcement units, Customs Enforcement and Coast Guard Command provide access to information and databases related to their fields of duty within the framework

of protocols signed with the relevant institutions. Information is exchanged between institutions thanks to these protocols.

403. For TF investigations, specific programs are used by GGC Counter-Terrorism Department (GGC-TEM) personnel to access financial information in a timely manner. In this context, through the KAFES programme they access dates of entry/exit of the person/suspect at the country's land borders, the amount and type of cash being carried, flight entry/exit information, identification of persons traveling with them, membership information of foundations/associations, to social security institution records and job data in real time. Through the JABS system they also access information's like individual/suspect's criminal records obtained from UYAP/KİHBİ data, current address, prison entry and exit information and vehicle ownership information. Twelve other programmes are used to examine financial analysis reports obtained from the FIU and to understand the relationship between money transfers and other transactions between individuals/suspects. In addition, GGC (KOM- Fight against Smuggling and Organised Crime) makes use of PARS analyses system that provides them with similar features.

404. For combatting customs smuggling, CEcan access directly the license Plate Recognition System (under a protocol with the TNP); the Vessel Tracking Module (Ministry of Transport); the Port Single Window System; the Decision Support System; the Intelligence Information System; as well as the Automation data of fuel distribution companies transmitted to the Ministry and relevant combatting agencies by the Energy Market Regulatory Authority (EMRA). The GIBINTRANET system (used by Revenue Experts) provides them with access to fiscal data. When filling in a Cash Declaration Form or Cash Disclosure Form, the passenger is requested to provide information and documents verifying the source of the cash (e.g. customs declaration or contract, proforma invoice, invoice, etc., for cash declared as export proceeds) all of them are registered under the Customs Enforcement data base. Customs Enforcement can also access information from other relevant public institutions through protocols and verified via the Cash Control Program, which provides convenience to the personnel entering the data and ensures the reliability of the shared information.

405. Information regarding individuals, companies, goods, and vehicles reported to Public Prosecutor's Office by the Directorate General is recorded within 24 hours in the Smuggling Information Database for tracking purposes. The unit manager reviews all information that authorised officials enter the Smuggling Information Database, if the information is deemed appropriate the entry is approved and transferred to the system. Information regarding individuals, goods, vehicles, and companies involved in smuggling incidents is also periodically queried by personnel responsible for the program at the Directorate General, and any existing deficiencies are completed based on new information received through feedback.

406. Furthermore, a wide range of data is provided to the competent authorities in an accurate and up-to-date format thanks to the TNP's EKİP-UYAP system integrations, INTERPOL channels, and the Gendarmerie's JİKİP-UYAP system integrations. For example, to verify that the information obtained is accurate and up-to-date, LEAs correspond with official institutions such as the Directorate General of Civil Aviation, the TRA, the Directorate General of Land Registry and Cadastre, the Turkish Banks Association and the Turkish Notaries Association. Also, the data from different sources, including MASAK, is analysed by LEAs using analysis programmes (Asena, Kafes, Ataç, I2, etc.) to support the production of intelligence which is then effectively utilised during investigations.

6.2. Production and dissemination of financial intelligence

6.2.1. Production of financial intelligence

407. Türkiye has a robust system to produce good quality financial intelligence and all other relevant information to appropriately support competent authorities' operational needs when conducting ML, associate predicate offences and TF investigation and prosecutions.

408. MASAK operations are divided into sixteen departments consisting of 249 analysts supporting their activities which is considered adequate. Eight departments produce different financial intelligence products depending on the stages of the analysis, from which two departments are responsible for STR analysis: (i) the Strategic Analysis Department, which performs bulk data analysis to guide other units; and (ii) the Operational Analysis Department, which manages STR data and co-ordinates efforts related to ML/TF cases.

409. Two other departments are specialised in TF analysis, one focusing on UN-listed terrorist organisations (ISIL, Al-Qaida and associate affiliates) and other terrorist groups exploiting religion, and another dedicated to PKK/KCK-PYD/YPG. Both departments also analyse cases related to FETÖ and other organisation. The table below demonstrates MASAK's number of files subject to further analysis in both, the TF Analysis and Evaluation Departments which demonstrates their ability to produce several types of financial intelligence products prioritising on of their main high-risk offences.

Table 6.3. MASAK TF reports disseminated to competent authorities (2021-2025)*

Year	Financial Analysis Report	Financial Detection Report	Information Note	Raw Data (CDs)	Total TF files/year
2021	5543	92	148	9080	14863
2022	3756	26	177	1621	5580
2023	2514	31	173	1209	3927
2024	2762	47	141	1440	4390
2025**	2245	70	246	122	2683
Total	**16820**	**266**	**885**	**13472**	**31443**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

410. Reporting entities submit STRs online. All STRs received by MASAK are reviewed on daily basis. An automated scoring system was implemented in 2021, and machine learning techniques were introduced in 2025. From 2021 to 2025, the scoring system was rule-based, generating index values from numerical and text-derived parameters (i.e., number of natural and legal persons mentioned in the STR; amount of the transaction; matching files and warnings in the data base; Egmont information requests, among others). Scores were calculated as raw values without statistical scaling. In 2025, MASAK implemented an EMIS-based AI system which has proven to accelerate the scoring system and improve the quality of the STRs categorisation, accelerating its preliminary analysis to then be disseminated to the respective departments.

411. This EMIS-based AI system, will score all STRs as 'normal', 'urgent' or 'highly urgent' based on indicators developed by MASAK staff and the underlying predicate offence reported in the STR. The model converts the binary classification output into a score between 0 and 100 using min-max scaling, referred to as the model score. The system will also categorise those STRs including a postponement of transaction. This scoring mechanism incorporates descriptions of suspicious transactions, history above a defined threshold, aggregate value of large money transfers, high-value payments to e-money institutions, and significant transfers to VASPs by using 632 terms in the model training and scoring generation and have proven to facilitate experts STRs revision once the preliminary scoring process is finished.

412. A dedicated group of 10 experts will review on daily basis those STRs categorised as 'urgent' and 'highly urgent' or requiring a postponement of transaction (approximately 1700 per day). FIU analysts provide their views on the assigned score and delegate them to the relevant departments for further analysis if needed. The Strategic Analysis Department directly analyses and assesses all TF and PF-related STRs and those categorised as 'urgent' and 'highly urgent'. As expressed in the table below, from a total of 2.7 M received STRs the majority are categorised as normal (91%). The AI-generated system categorises only a small proportion of STRs as urgent (6%), highly urgent (less than 1%) or as requesting a postponement of transaction (2%) at the entry level reflecting the capacity of experts to review these STRs on daily basis.

Table 6.4. STRs overall scoring (2020-2025)

Year	Normal	Urgent	Highly Urgent	STRs with request for postponement of transaction	Total
2020	209324	20385	1276	6546	**237531**
2021	473371	23292	1114	7218	**504995**
2022	389105	30351	959	4907	**425322**
2023	540554	44798	761	15442	**601555**
2024	508853	33415	559	15768	**558595**
2025*	382959	16201	440	12734	**412334**
Total	**2504166**	**168442**	**5109**	**62615**	**2740332**

Note: (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

413. When the group of experts reviews the preliminary scoring, they are able to electronically cross-check all the information submitted in the STR against the data bases and produce a preliminary report indicating all the available information related to the natural or legal persons reported and if information related to a previous STR matches the information, submitted in the new one, the previous STR is linked to the new one and referenced for further analysis. The expert's revision of the preliminary scoring system enables MASAK to revisit STRs initially rated as normal or urgent for deeper analysis later, minimising overlooked information and ensuring its effective use.

414. From the total STRs received, MASAK analysed 1.2 million STRs (46%) mostly as part of their strategic analysis work. This number is significantly higher than those MASAK is required to review during the scoring process, which only represents the 8% of the total submitted STRs. However, only 228 770 STRs (16%) out of all STRs were used for ML, TF, and predicate offences operational analysis and examination which remains modest given the large number of STRs received. MASAK proactively opened 360 files for case relation search, which included searches on approximately 218 000 individuals. Most of these files are related to illegal betting and gambling (18%), fraud (11%), tax evasion (7%) which is generally aligned with the country's risk profile. Although the number of TF-related files seems limited (3%) compared to the overall number of opened files, competent authorities have confirmed that all TF-related STRs are analysed by the two TF analysis departments.

415. MASAK analyses STRs and other relevant information and produces strategic and operational analysis. It also carries out risk and sectoral studies regarding emerging developments on the field of laundering proceeds of crime (i.e., cash smuggling, misuse of e-market place, drugs, fraud, and misuse of cryptocurrency), and TF. MASAK produces ML/TF analysis and evaluations reports at a policy level and strategic analysis reports aiming at identifying and detecting activities of large and organised criminal networks. Whereas at an operational level, MASAK produces four types of financial intelligence reports for ML-related cases: financial analysis report (FAR), financial detection report (FDR), proceeds of crime reports (PCR) and informative reports (IR). MASAK has the ability to identify and trace complex ML/TF cases,

identifying criminal networks using a combination of different channels to launder proceeds of crimes and finance terrorist activities (i.e. misuse nominee, shell companies, real estate, and unhosted VA wallet).

416. To produce these wide range of analysis and reports, MASAK uses several IT tools (EMIS, MOS, NPL, among others) which allows MASAK to connect all data available in Türkiye's data bases and produce robust intelligence reports to be disseminated to the relevant competent authorities. The table below shows the number of files opened for further analysis within the scope of the work of the FIU confirming that most of the analysis work is orientated towards TF files (76.4%) compared to ML/PO files (23.6%).

Table 6.5. Files opened for further financial analysis (2020-2025)*

Year	ML/PO files	TF files	Total files/year
2020	1223	10261	11484
2021	1133	6631	7764
2022	1446	5508	6954
2023	1665	4011	5676
2024	2071	4283	6354
2025*	2472	2226	4698
Total files opened/offence	**10010**	**32920**	**42930**

Note: (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

6.2.2. Dissemination of financial intelligence

417. MASAK disseminates financial intelligence to different competent authorities spontaneously (proactive dissemination) or upon request (reactive dissemination). Each dissemination file is built on a comprehensive analysis with the financial profile of every reported individual, intelligence emanating from multiple STRs and all other financial data available in the MASAK's database.

418. The FIU prepares different type of reports for dissemination: (i) the FAR is disseminated to judicial authorities answering to their requests or informing a suspicious of a criminal activity; (ii) the FDR is prepared after the finishing the verification of the transactions subject to postponement and is disseminated to judicial authorities for seizure purposes; (iii) the PCR informs the judicial authorities on the available assets or funds for preparation and planning of a seizure; (iv) IR are prepared within the scope of opened files to share the files analysis results with relevant authorities, typically after file completion; (v) ML/TF analysis and evaluation reports analyses trends and/or specific cases on either offences; (vi) CD reports are disseminated in urgent cases containing raw data on a specific event being investigated and are mainly distributed for disruption purposes.

419. Between 2021 and 2025, MASAK disseminated 7 679 files related to ML or associated predicate offences (ML/PO), 48% proactively (3 683 files) and 52% reactively (3 996 files), demonstrating a balanced approach and strong capability to produce and share financial intelligence. Proactive dissemination has incremented in a 72% from 2021 to 2025, which also reflects the MASAK's efforts in the use of financial intelligence. In this context, 3 060 files related to aggravated fraud/fraud (42%) and 1 808 on illegal betting (25%) were disseminated, which represents a 67% ratio of the total disseminated reports in alignment with the top two predicate offences in the country. However, dissemination of other high or medium-high risk predicate offences remains limited (i.e. 634 files for drug trafficking; 249 for smuggling; and 275 for migrant smuggling/human trafficking) which does not align with the country's risk profile. The table below indicates the type of reports disseminated:

Table 6.6. MASAK ML/PO reports disseminated to competent authorities (2021-2025)*

REACTIVE DISSEMINATION									
Year	**ML examination**	**PCR**	**FAR**	**ML Evaluation**	**IR**	**CD Report** (Raw data)	**FDR**	**Formal Letter/Other**	**Total**
2021	40	177	61	71	4	104	28	0	**485**
2022	44	197	53	123	7	127	11	5	**567**
2023	31	126	152	190	4	13	13	4	**533**
2024	35	108	389	554	2	2	0	0	**1090**
2025**	59	83	426	719	31	1	0	2	**1321**
Total	209	691	1081	1657	48	247	52	11	3996
PROACTIVE DISSEMINATION									
2021	0	0	0	0	321	0	294	0	**615**
2022	0	0	27	3	485	0	198	11	**724**
2023	0	0	117	9	404	2	125	0	**657**
2024	0	0	361	0	47	0	193	21	**622**
2025	0	0	389	0	101	0	575	0	**1065**
Total	0	0	894	12	1358	2	1385	32	3683
OVERALL DISSEMINATION									
TOTAL	209	691	1975	1669	1406	249	1437	43	**7679**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

420. MASAK also disseminated a total of 31 443 files related to terrorism and TF, 2.5% proactively (796 files) and 97.5% reactively (30 647 files). Although proactive dissemination has incremented in 56% form 2021-2025, the low rate of proactive TF disseminations reflects that most investigations stem from intelligence and terrorism cases, making MASAK's approach largely reactive to the analysis of TF files. The high ratio of reactive dissemination signals limited detection of TF-related suspicions transactions in MASAK's databases prior to judicial requests, though such requests enable the MASAK to connect the necessary links during investigations and provide high quality reports.

Table 6.7 MASAK TF reports disseminated to competent authorities (2021-2025)*

Year*	**FAR**		**FDR**		**IR**		**CR Report (Raw data)**		**Total disseminated reports/Year**
	Reactive	**Proactive**	**Reactive**	**Proactive**	**Reactive**	**Proactive**	**Reactive**	**Proactive**	
2021	5536	7	0	92	133	15	9077	3	**14863**
2022	3726	30	0	26	136	41	1619	2	**5580**
2023	2507	7	0	31	113	60	1206	3	**3927**
2024	2755	7	0	47	58	83	1437	3	**4390**
2025**	2181	64	0	70	48	198	119	3	**2683**
Total	**16705**	**115**	**0**	**266**	**488**	**397**	**13458**	**14**	**31443**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

421. MASAK disseminated 26 774 TF products related to FETÖ (85%), 2 842 related to terrorist organisations abusing religion (9%), 1 445 related to PKK/KCK-PYD/YPG (5%), 164 related to leftist organisations (less than 1%) and 218 related to other TOs(less than 1%). Proactive disseminations are more balanced as 672 files were disseminated in relation to terrorist organisations abusing religion (34%), 187

FETÖ (28%), 119 PKK/KCK-PYD/YPG (18%) and 133 on other TO (20%) which is align to the country's risk profile to some extent.

422. All competent authorities highlighted the role, the quality and the timing of the MASAK's financial analysis to pursue complex ML/TF/PF investigations including with transnational element, which was confirmed through case studies. MASAK has considerably improved the dissemination of financial intelligence reports upon judicial requests to an average time of 2 weeks, even lesser, by utilising digital transformation which has been highly noted by public prosecutors and LEAs. As a member of Egmont Group, the production and dissemination of financial intelligence have also benefited from information exchanges with other FIUs (see IO.2).

6.2.3. FIU financial intelligence supporting needs of competent authorities

423. The financial intelligence produced by the MASAK largely contributes to support the needs of competent authorities at an operational level. Between 2021-2025, MASAK disseminated a total of 39 620 reports to other competent authorities, mainly to judicial authorities (85%), including prosecutors, and to a lesser extent to LEAs (11%), supervisory authorities and other relevant ministries (3%) and other intelligence units (1%). The large number of reports disseminated to judicial authorities is consistent Türkiye's institutional framework and the fact that public prosecutors lead ML/TF investigations and courts are deciding on seizure and confiscating measures.

Table 6.8. MASAK overall dissemination to competent authorities (2021-2025)*

Competent authorities	PCR	FAR	Examination	ML evaluation	IR	FDR	CD (raw data)	Other	Total files/authority
ML/PO-RELATED FILES									
Judicial authorities	1282	485	198	1187	683	1511	246	62	5654
LEAs	8	503	10	3	912	43	3	5	1487
Supervisory authorities	0	153	1	2	413	60	0	8	637
Other Ministries	0	15	0	0	116	8	0	3	142
MASAK	4	22	0	2	93	11	0	17	149
Intelligence Units	0	16	0	0	61	3	0	1	81
Total ML/PO-related files	**1294**	**1194**	**209**	**1194**	**2278**	**1636**	**249**	**96**	**8150**
TF-RELATED FILES									
Judicial authorities	0	15868	19	0	83	247	11897	0	28114
LEAs	0	837	0	0	403	41	1524	0	2805
Intelligence units	0	5	0	0	80	21	9	0	115
Other (relevant ministries supervisory authorities, etc.)	0	85	5	0	333	4	9	0	436
Total TF-related files	**0**	**16795**	**24**	**0**	**899**	**313**	**13439**	**0**	**31470**
TOTAL NUMBER OF FILES									
Total files	**1294**	**17898**	**233**	**1194**	**3177**	**1949**	**13688**	**96**	**39620**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

424. Between 2021 and 2025, the 37.5% of MASAK disseminations (16 758 files) triggered ML/TF investigations (see IO.7), with most reports either initiating new investigations (68%), supporting ongoing cases (9%) and meeting other LEAs needs (7%). MASAK products also assist tax and supervisory authorities for audits, complaints, and administrative sanctions. While MASAK collaborates closely with prosecutors and LEAs throughout investigations and uses working groups to share expertise, there is no clear mechanism to monitor the quality of disseminated intelligence. Additionally, MASAK conducts regular

statistical and strategic analyses of STRs to help operational authorities in the timely detection of new trends. Below, this is exemplified by a case on a strategic analysis conducted on ML case abusing social media.

Box 6.1. Broadcast: MASAK's proactive financial intelligence dissemination resulting in enforcement actions

Operation BROADCAST was launched following the MASAK's dissemination of a financial detection report to public prosecutors, triggering a nationwide crackdown. The case involves stand-alone money laundering using VASP, credit cards, virtual POS systems, and MVTS, and is currently at the prosecution stage.

In June 2023, MASAK detected suspicious ML activity patterns emerging on a popular social media platform. By leveraging its analytical capabilities, MASAK examined over 4 000 bank account movements, identifying links to crimes such as fraud via information systems, misuse of bank and credit cards, money laundering and establishing an organisation for committing crimes. The transaction volumes among the suspects were approximately EUR 34 M.

Once the intelligence was consolidated, MASAK activated its dissemination mechanisms. Detailed reports and actionable intelligence were shared with law enforcement and judicial authorities through secure channels, enabling rapid co-ordination. This collaboration culminated in simultaneous operations across 37 provinces. In 2023, 164 suspects were taken into custody.

MASAK also provided comprehensive asset-tracing intelligence, leading to the seizure of real estate (38 apartments), vehicles (38), shares of 14 companies, bank and VAs accounts (1 700), and cash—valued at approximately EUR 18 M. These seizures were possible because the MASAK's information flow ensured prosecutors and courts had the evidence needed to act decisively.

6.2.4. Other competent authorities producing financial intelligence (where relevant)

425. LEAs produces financial intelligence to conduct their prevention duties and upon prosecutors' requests. Prosecutors mainly rely on MASAK financial analysis to support complex cases as they have direct access to all types of financial information and better staff specialisation. TNP and GGC can produce financial intelligence based on their databases and can request other competent authorities to provide financial information if needed. In addition, LEAs uses specialised programmes to examine financial analysis reports obtained from MASAK and to understand the relationship between money transfers and other transactions between individuals/suspects. For example, GGC (KOM- Fight against Smuggling and Organised Crime) makes use of PARS analyses system.

6.3. Co-operation and exchange of information/financial intelligence

6.3.1. Co-operation and exchange

426. Türkiye's competent authorities have close formal and informal co-operation mechanisms in place to exchange financial intelligence and other relevant information to pursue ML/TF investigations and prosecutions. Through different case studies, public prosecutors, LEAs (in particular, TNP and GGC) and MASAK have demonstrated to formally share information on daily basis through the UYAP system but also through case-specific strategy co-ordination round tables. Close ad hoc and formal interagency co-operation mechanisms between MASAK and competent authorities have proven to facilitate the exchange

of financial intelligence leading to the disruption of large criminal networks and high-impact outcomes on investigations.

427. Due to MASAK's pivotal role in the AML/CFT/CPF system, they received 9 600 information sharing requests and fulfilled 5 628 (59%) between 2020 and2025. From which, the majority corresponds to information sharing requests from public prosecutors (41%), TNP (24%) and other ministries (12%), indicating the fluid interagency exchange of information for operational purposes. MASAK's prioritises TF and urgent operations requests but also has an established prioritisation system based on the risk country profile. All competent authorities highlighted the role, quality and timing of MASAK's responses as adding great value to pursue complex ML/TF/PF investigations including with transnational element.

Table 6.9. MASAK's number of initiated and fulfilled information sharing requests (2020-2025)

Requesting competent authority	2020		2021		2022		2023		2024		2025**	
	Initiated*	fulfilled	initiated	fulfilled	initiated	fulfilled	initiated	fulfilled	initiated	fulfilled	initiated	fulfilled
PPO	479	237	1804	370	280	277	318	193	412	262	671	308
Ministries	123	209	189	287	145	275	181	222	161	205	130	203
TNP	269	99	287	110	342	124	437	115	523	151	428	86
Courts	50	72	344	181	90	120	34	48	44	89	62	81
TIB	16	11	19	43	22	41	18	16	12	31	21	50
CMB	76	21	129	24	125	65	93	52	72	13	31	5
CBRT	8	13	18	16	16	20	14	21	22	33	23	44
Customs Enforcement	2	2	18	16	15	50	7	16	1	3	2	5
GGC	11	0	11	4	16	9	32	5	42	21	39	7
BRSA	12	20	15	6	12	1	6	7	8	4	3	3
Other	36	71	85	95	139	130	155	93	179	103	216	114
Total	**1082**	**755**	**2919**	**1152**	**1202**	**1112**	**1295**	**788**	**1476**	**915**	**1626**	**906**

Note: (*) the numbers under the "initiated" category may also include letters received in response to request for information sharing submitted by MASAK to competent authorities; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

428. Through the signature of 32 MoUs, MASAK can directly access other 32 competent authorities' databases (i.e., TNP, MoI, MoT, MoJ, Risk centre of Banks Association in Türkiye, among others), which also enhances the exchange of information for the development of financial intelligence and creates a robust roster of information. TNP and GGC also have direct access other competent authorities' databases and information systems such as UYAP, KPS, DERBIS and VBYS Among other LEAs, CE and CGC provide access to information and databases related to their fields of duty within the framework of protocols signed with the relevant institutions. Information is exchanged between institutions thanks to these protocols.

429. All LEAs can form joint task forces for a specific case or an issue. For example, a joint task force has been established under customs to combat fuel smuggling with the involvement of TNP, GGC, and TIB and MASAK. Specialised public prosecutors discuss complex cases with the FIU in daily basis, and all LEAs, prosecutors and MASAK can and do form joint investigation teams for specific cases or the study of an emerging trend. Even MASAK's officials have been temporarily assigned to work on LEAs offices when the complexity of the case required it.

430. Furthermore, competent authorities can exchange of information with its foreign counterparts either through a liaison officer or secure international IT system (such as Egmont Secure Web), encrypted communication for non-Egmont member, or as members specific operational networks (such as CARIN and INTERPOL).

6.3.2. Security and confidentiality

431. To protect the information's confidentiality, competent authorities exchange the information through encrypted integrated judicial information systems. During investigations, all competent authorities are obliged not to disclose any information attained by FIU staff, examiners and members of CBCFC during their in-service activities.

432. All information subject to dissemination are considered as official documents and are subject to confidentiality measures. Both MASAK and competent authorities apply robust legal, technical, and operational safeguards to ensure that all exchanged information is protected by strict confidentiality and used securely and appropriately. For example, MASAK's products that are disseminated to the competent authorities through the UYAP system, Recorded Electronic Post System (KEP) and BELGENET, or by post depending on their level of importance. Furthermore, the FIU keeps its IT systems up to date to prevent leaks of information and have also established protocols to exchange information with FIs and DNFBPs supervisory authorities, which has been certified through TS ISO/IEC 27001, including physical environment and data security. MASAK stores data in both the database and an isolated network infrastructure and have established a disaster recovery program with high security protocol.

433. MASAK secures the information based on three pillars:

a) Information security processes: established information security policies to protect confidentiality, integrity, and availability of assets, supported by ISO 27001-based risk management, continuity plans, and awareness activities. A multi-layered security approach was implemented, including user authentication, IT infrastructure protection, network security, and continuous monitoring and audits.
b) Security of physical environments: access to IT areas and the data centre is strictly controlled through ID cards, face recognition, and supervision, with all entries recorded. The data centre is secured with physical barriers, fire protection, environmental monitoring, redundant systems, and a separate business continuity site. Confidential documents are locked, visitor access is restricted, and personnel follow Clean Desk policies, ensuring security and operational continuity.
c) Data security: the access to information is categorised and limited based on functional groups and departmental hierarchy, ensuring role-specific permissions and controlled workflows. Information sharing is secured through electronic systems like KEP, MOS, BELGENET, and ESW, with strict confidentiality protocols. Encryption using symmetric and public keys protects data integrity during exchanges with judicial authorities and FIUs. Other additional security measures include closing USB ports, administrator-controlled file transfers, and monitored personal folders for secure internal and external sharing.

434. Other competent authorities can request information from MASAK data base through the UYAP system, which contains encryptions features to guarantee the confidentiality when transmitting the information. However, it is not clear how the information is preserved once disseminated to other authorities.

435. All competent authorities involved in joint investigation processes adhere to the correspondence procedures outlined within the scope of the Regulation on the Procedure of Official Correspondence. The institutions constituting the task force distribute the information and documents they have prepared as hard copies or soft copies based on confidentiality levels, and in addition, the relevant institutions are required to carry out the necessary IT infrastructure for the protection of this information and documents.

6.4. Using information/financial intelligence

6.4.1. Using information / financial intelligence for investigations and developing evidence

436. Türkiye uses financial intelligence and other relevant financial information to a very large extent pursuing positive results when investigating and prosecuting ML, associate predicate offences and TF. This was demonstrated through several case studies where financial intelligence is being translated into concrete enforcement actions to pursue investigations and prosecutions.

437. To achieve these results, competent authorities are using various and broad range of financial intelligence and information (e.g., MASAK's report, denunciation, public institutions information, and foreign counterparts). Between 2021 and 2025, MASAK disseminated a total of 8 150 ML and/or associated predicate offences report and a total of 31 470 TF related reports (see table 6.8) to competent authorities. The ratio of the total number ML cases opened after MASAK's dissemination is approximately 37.5%, from which approximately 75% ends in conviction which confirms the high-level of utility of financial intelligence products.

438. Other competent authorities, have used MASAK's financial intelligence and information reports for the following purposes:

a) LEAs: start of a new research and/or investigation (68%); assessment phase (16%); ongoing research and investigation (9%); acquiring information for LEAs operational needs (7%).
b) TIB: imposition of fines related to tax or other administrative matters on the persons subject to reporting (37%); opening new tax checks, audits and reviews (25%); use for further analysis on ongoing tax checks, audits and reviews (25%); filling criminal complaints against the person subject to report (11%); other (2%).
c) Supervisory authorities (BRSA, CMB, CBRT, etc): opening new inspections, audits and reviews (32%); ongoing inspections, audits and reviews (8%); filling criminal complaint against the person subject to MASAK investigation (22%); imposition of administrative fines (12%) and other purposes (26%).

6.4.2. Using information / financial intelligence to assist in identifying and tracing criminal proceeds or instrumentalities

439. Türkiye makes a good use of information and financial intelligence to assist and trace proceeds or instrumentalities which is progressively resulting in seizures and confiscations (see IO.8). The FIU produces specific proceeds of crime report including financial intelligence on the links between possible proceeds of crime and the assets of individuals or third parties, identify proceeds of crime that can be seized and confiscated through its analysis, and share this information with public prosecutors and judges.

440. Competent authorities have used FIU information and financial intelligence products to identify and trace criminal property and property of corresponding value in 1 197 cases (See 8.2 and 8.3). Between 2021 and 2025, 612 cases triggered seizure of assets for a total of EUR 147 M and confiscation of assets for EUR 93 M. Furthermore, the criminal complaints of MASAK can also be considered within the scope of evidence development. In this respect, following the freezing orders, criminal complaints for TF were filed against all 1 434 individuals (see 10.1) and criminal investigations were initiated against 342 individuals for TF offence (see 9.1).

7 Money laundering investigations and prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.7. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 3, 30, 31 and elements of R.1, 2, 15, 32, 37, 39 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Türkiye has an appropriate legal and operational framework to identify and investigate all types of ML activities domestically, including through parallel financial investigations. Türkiye's competent authorities identify ML activities utilising a wide range of information and investigative tools. ML investigations are generally triggered by referrals from other competent authorities (i.e., MASAK), LEAs operational work and information from foreign counterparts. However, the limited numbers of investigations triggered by CE remains a concern given the risks of cross-border currency movement, high levels of smuggling and transnational drug trafficking.

b) Competent authorities can identify foreign-linked ML activities triggered by domestic predicate offences investigations and information from foreign counterparts to a large extent, particularly related to fraud, drug trafficking and illegal betting. Türkiye develops foreign-linked ML investigations by having solid channels of communication with LEAs counterparts, Interpol and Europol, as well as liaison officers (see IO.2). Türkiye identifies ML or predicate offences with any type of nexus to the country as domestic offences for investigation purposes. For this reason, the majority of ML investigations are triggered by domestic predicate offences, including foreign elements (97%)

c) Specialised ML public prosecutors play a leading role in ML investigations. Public prosecutors are appropriately and adequately skilled, with 15 dedicated AML Prosecutor's Bureaus located in the metropolitan cities, and highly trained to pursue both ML investigations and predicate crime offences-related investigations. Public prosecutors are operationally supported by LEAs, primarily by specialised units within the TNP and GGC, which are well-resourced and trained, while support from CE and the CGC remains more limited given their competences, particularly tailored to the detection and identification of cross-border cash and currency movement, high

levels of smuggling, and transnational drug trafficking. Public prosecutors and LEAs mainly rely on MASAK to produce financial analysis reports to serve pursuing ML investigations.

d) Public prosecutors opened approximately 23 184 ML investigations, with a significant surge in 2024 (33%) and 2025 (43%), due to the increase in awareness and specialisation of LEAs and the creation of PPOs ML Bureaus. However, given Türkiye's contextual and material factors (i.e., size of the financial sector, geographical position as a transit hub, the extent of cash-based and size of informal economy) ML investigations, prosecutions and convictions in high-risk areas other than fraud (i.e., professional ML, misuse of legal persons, and cash cross-border movements) (see IO.1) is more limited.

e) Fraud (including aggravated fraud) is the most relevant predicate offence of ML with total 16 586 cases (80%), followed by a low number of investigations in other high and medium risk predicate offences, such as illegal betting with 1 428 (7%), drug trafficking with 1 267 cases (7%), customs smuggling with 590 cases (3%) which is not aligned with the country's risk profile.

f) Türkiye identifies all type of ML activities in investigations, prosecutions and convictions. Most of the cases reaching conviction are related to self-laundering (55%), followed by third-party ML (26%), and a combination of both in the remaining cases (19%) including effective stand-alone ML related to illegal betting.

g) Türkiye has progressively incremented ML prosecutions achieving 10 581 prosecutions and 556 convictions for ML offences during the reporting period, with a significant increase during years 2024 and 2025. Türkiye has shown ability to conduct complex ML investigations. There are nevertheless challenges in fully translating investigations into judicial outcomes which generates a backlog in the number of pending prosecutions (7248 cases) and convictions (6 085), comprising to a less extent prosecution and conviction on complex ML that involved professionals (9%). To increase the pace of ML prosecution and conviction, in 2023, Türkiye's established a specialised ML court. However, challenges remained related to the lack of ML training and expertise of judges and prosecutors on complex ML, the non-systematic use of financial analysis during investigation and prosecution phases despite being mandatory and the need for further guidance to prosecutors and judges related to how to prove knowledge and intent through circumstantial evidence as it has negatively impacted achieving ML convictions.

h) ML sanctions for natural persons are proportionate, effective and dissuasive in general. The sentencing range is approximately four years and four months of imprisonment which is considered higher than for other serious offences. However, when the ML offence is coupled with the intervention of public officials in the criminal activity, professional money launderers and/or organised crime the imprisonment sanctions are not dissuasive. Although legal persons cannot be subject to criminal sanctions due to Türkiye's fundamental principles of domestic law, they can apply other administrative sanctions. Türkiye demonstrated the applications of such sanctions in the context of criminal investigations in limited cases which is not effective nor dissuasive.

i) Türkiye applies alternative measures when securing an ML conviction is not feasible, provided evidentiary standards are met (e.g., pursuing tax evasion or other predicate offences). However, competent authorities have not clearly demonstrated how these measures are applied as an alternative measure.

Key Recommended Actions (KRAs)

m) Further prioritise ML investigations and prosecutions related to certain high-risk predicate offences (drug trafficking, smuggling and illegal betting) that involve complex ML cases, particularly linked to high-risk activities (professional ML, goods and cross-border movement of currency, misuse of legal persons).

n) Develop clear guidelines for ML prioritising prosecutions in line with Türkiye's risk profile with the aim of reducing the backlog of pending prosecutions.

o) Enhance the consistent application of sanction against natural and legal persons convicted for ML to ensure they are effective and dissuasive, particularly in cases involving public officials in the criminal activity, professional money launderers and organised crime.

Other Recommended Actions

a) Prioritise and expand ML investigations involving cash border movements, unlicensed intermediaries (such as hawala and foreign exchange operators), and the misuse of legal persons, including cases involving facilitation by accounting and legal professionals.

b) Expand ML investigation related to stand-alone ML to other predicate offences.

Overall Conclusions on IO.7

Türkiye has established an appropriate legal and operational framework to identify and investigate a wide range of ML activities at a domestic level, including those categorised as domestic ML with foreign elements.

Public prosecutors leading ML investigations are generally well resourced and specialised and systematically conduct parallel financial investigations supported by LEAs to different degree based on their areas of competences. However, public prosecutors and LEAs often delegate the financial analysis in complex cases to MASAK due to its level of expertise signalling the need to enhance LEAs capabilities to support parallel financial investigations.

Türkiye opened 23 184 ML investigations, which partly align with the country's risk profile given Türkiye's contextual and material factors (i.e., size of the financial sector, geographical position as a transit hub and size of informal economy) and ML investigations, prosecutions and convictions in high-risk areas other than fraud (i.e., professional ML, misuse of legal persons, and cash cross-border movement) (see IO.1) is more limited, with a noticeable increase in 2024 (33%) and 2025 (43%), driven by greater awareness, specialization, and the creation of PPO ML Bureaus. Fraud-related offences dominate as predicates while investigations into other high-risk crimes, such as illegal betting, drug trafficking, and customs smuggling, remain disproportionately low compared to the country's risk profile.

Türkiye has progressively incremented ML prosecutions achieving 10 581 prosecutions and 556 convictions for ML offences and has shown ability to conduct complex ML investigations reaching prosecution stages using several and sophisticated investigative tools. To increase the pace of ML prosecution and conviction, in 2023, Türkiye established a specialised ML court. However, public prosecutors present challenges when demonstrating *mens rea* to achieve conviction in complex ML cases, this coupled with a high-level ratio of pending prosecutions, indicates the need for further and strategic prioritisation of complex ML cases.

Most convictions involve self-laundering (55%), followed by third-party ML (26%) and mixed cases (19%). However, investigations and convictions linked to foreign predicate offences are minimal, despite Türkiye's role as a transit hub for funds and goods.

Sentencing ranges are proportionate, effective and generally dissuasive for natural persons. In ML cases involving public officials in the criminal activity, professional money launderers and organised crime sentences ranges are not dissuasive. Despite being able to apply administrative sanctions to legal persons, these measures have been applied to 18 legal entities, which is disproportionate to the country's risk profile, where most cases indicate the systematic abuse of legal entities in complex, multi-layered ML schemes.

Türkiye is rated as having a Moderate level of effectiveness for IO.7.

Immediate Outcome 7

7.1. ML activity identified and investigated

441. Türkiye identifies and investigates all types of ML activities, including through PFIs to a large extent. Türkiye demonstrated through case studies their ability to identify and investigate ML activities in all stages. In general, cases triggering investigations are typically related to cash deposits into bank accounts, followed by the use MVTS (licensed or unlicensed), VASPs and money mules. While layering techniques are investigated to a lesser extent, with typologies including the creation of multiple small business and companies, professional ML (i.e., through lawyers and accountants) and TBML, ultimately, the purchase of real estate and gold, and the creation of small business and enterprises are recognised as the main integration mechanisms in most ML investigations. Türkiye's remaining challenges appear related to the detection and identification ML activities through cross-border currency movements which does not align with Türkiye's risk profile given the country's position as a transit hub for funds and goods, including concerning the abuse of cash-based intensive in Türkiye (see IO.1).

442. ML activities are generally identified through public prosecutors predicate offences investigations, LEAs operational work and the FIU financial analysis. Complex ML schemes are generally triggered by domestic predicate offences investigations and international requests. Türkiye identifies and investigates ML through different mechanisms, including from the dissemination of FIU reports (37,5%) (see IO.6), LEAs intelligence information, denunciation from other competent authorities, foreign counterparts' international co-operation (see IO.2) and victims' denunciation.

443. When ML activities are detected LEAs, intelligence units, and MASAK immediately shares the findings of suspicious laundering activities with the PPOs, who will direct the investigation ensuring a unified and co-ordinated action. As a civil law jurisdiction, the public prosecutor will lead the investigation supported by LEAs. This centralized approach enables co-ordinated inquiries into both the predicate crime and ML offences. In the metropolitan cities, Specialised ML prosecutors lead ML investigations supported by LEAS specialised units (TNP and GGC) while in the rest of the cities, investigations can be led by public prosecutors. Since 2021, public prosecutors are required to initiate parallel financial investigations after even the slightest suspicion of ML following Türkiye's national policy on ML investigations and prosecutions and mandatory Circular issued to all Prosecutors. However, despite the growth of ML investigations and prosecutions has recently increased some challenges remain on how judicial authorities proves knowledge and intent through circumstantial evidence which negatively impacted achieving ML convictions. Prosecutors and LEAs rely on the FIU financial intelligence and analysis for complex ML cases. When needed, public prosecutors can require support to the CGC and CE, intelligence units, supervisory and regulatory authorities.

444. To gather information, collect and produce evidence, public prosecutors can request information of all natural, legal persons and competent authorities in the context of an investigation. LEAs can access basic information and beneficial owner of legal persons through various channels (i.e., MERSIS, request to MASAK and Turkish Revenue Authority (TRA) and LEAs can obtain BO information from competent authorities. Interagency request of information is hosted in the UYAP system to guarantee the confidentiality during exchanges. Investigations are co-ordinated in a robust manner combining the use of special techniques of investigations and the creation of ad hoc interagency and international joint investigations teams, when needed due to the complexity of the case.

445. Türkiye has implemented mechanisms to identify ML activities and discuss new trends at an operational level based on the NRA findings. As part of the Threat WG duties, prosecutors, LEAs, intelligence agencies, FIU and all other relevant competent authorities regularly meet to discuss ML typologies, emerging trends and specific cases to exchange knowledge, develop new ML indicators and

best practices on disrupting ML activities. Since 2019, personnel from the TNP Narcotics, MASAK, foreign liaison officers, and public prosecutors have held approximately 350 meetings on investigation topics related to ML/TF. Although no specific information was provided to assess how many of these meetings were solely focused on ML specific cases, competent authorities explained they were mainly focused on drug trafficking-related ML crimes and, as a result, they issued 498 investigation orders covering 4 743 individuals and converted 129 preliminary investigations into operations which further demonstrates Türkiye's use of solid operational interagency co-operation mechanisms. There is no information has been provided the prioritization related to fraud, high-level smuggling, and illegal betting as high-risk predicate offences.

446. To support the development of investigations, competent authorities have designed several PFIs guidance (i.e., guidance published in 2025 by different units of GGC and TNP) complemented by MASAK's ML typologies reports for operational use (2023 and 2025). These documents are periodically updated and published, including the consolidation of case studies, best practices, and templates for interagency information sharing that LEAs have already implemented. This has led to a marked improvement in LEAs, prosecutors and MASAK staff's awareness, which in turn resulted in a substantial increase in the number of ML investigations conducted in 2024 and 2025. Prosecutors, supported by LEAs and MASAK, use these indicators to investigate ML schemes from simple cases to complex networks involving multiple predicate offences.

447. Türkiye also has mechanisms in place to identify foreign-linked ML activities through solid channels of communication with LEAs counterparts, Interpol and Europol, as well as liaison officers (see IO.2). Türkiye's majority of ML investigations are triggered by domestic predicate offences, including coupled with foreign elements (97%) although complex ML investigations involving professional and cross-border currency movement is more limited. The table below shows the differences between domestic ML investigations vs. those triggered by foreign counterpart requests.

Table 7.1. ML investigations per triggering source (domestic vs. foreign predicates offences)

Triggering source	Domestic ML investigations (*)	Foreign ML investigations	Total investigations	Ration of total ML investigations
Complaints from victims	1593	46	1639	7%
Referrals from other agencies	11044	319	11363	49%
Ex Officio (Foreign counterparts)	4797	138	4935	21%
LEAs	5100	147	5247	23%
Total	**22534**	**650**	**23184**	100%

Note: (*) Domestic ML investigation refers to cases where: (i) part of the predicate offence or the money-laundering conduct occurs in Türkiye; or (ii) the related financial flows pass through the Turkish financial system. In both scenarios, the cases are recorded as domestic ML investigations, notwithstanding the presence of foreign elements within the iter criminis.

448. Türkiye has a robust institutional and well-resourced framework to investigate ML and predicate offences. Public prosecutors lead ML investigations supports by all LEAs, and when the specificity of the case needs it, they can request MASAK experts' and other competent authorities for further analysis. Despite LEAs wide range of capacity and competences to support a criminal investigation, the limited numbers of investigations triggered by CE remains a concern given the country risks of cross-border currency movement, high levels of smuggling, and transnational drug trafficking.

449. PPOs operate in all 81 provinces of Türkiye independently. Each PPO is directed by a Chief Prosecutor who decides on the operational implementation of the national criminal policies designed by the MoJ. Since 2023, 15 PPOs have specialised ML Bureaus with at least one specialised ML prosecutor leading and co-ordinating ML investigations. These 15 PPOs are located in the metropolitan municipalities with the highest criminal indexes[31] where the allocation of ML specialised resources is needed. In addition, Türkiye has also implemented a prioritisation mechanism for ML cases in those remaining 10 PPOs metropolitan cities[32] where no specialised ML bureaus are established by requesting public prosecutors in charge of other units (i.e., organised crime) to prioritise ML cases at a 1/2 workload ratio, but the effectiveness of this instruction was not demonstrated. In the remaining 145 PPOs, prosecutors manage these cases at a 1/3 workload ratio. If needed, competent authorities can open more specialised units or assign a specialised ML prosecutor on case basis. When ML prosecutors conduct independent investigations alongside ongoing predicate crime inquiries, they co-ordinate closely with the prosecutor handling the predicate offence, obtaining necessary information to complete the laundering investigation. It was not possible to distinguish how many of these prosecutors intervene in during the investigation and prosecution phases.

450. To pursue effective investigations, the public prosecutor selects the appropriate specialized LEAs unit to handle the case and co-ordinates parallel financial investigations strategies through their ML bureaus. Public prosecutors can also request several LEAs to intervene in different enforcement actions based on LEAs competences, resources and expertise to accelerate investigations and ensuring effective enforcement outcomes.

a) The TNP has approximately 5 000 officials distributed within different specialised departments on investigating high and medium-high risk predicate offences. Most of them supports the implementation of enforcement actions and special techniques of investigations (i.e., control deliveries, search warrants, wiretapping, etc) in the field upon the prosecutor's request. Although all specialised departments can produce financial intelligence and/or analysis of the proceeds of crimes, it was not possible to assess the officials' level of expertise and effectiveness of the parallel financial investigations led by them and if they are sufficient to support the ML investigations needs. The specialised department are as follows:
    a. TNP KOM is present in all 81 provinces with different degrees of specialisation in combatting criminal proceeds. The department has 17 dedicated officials working in headquarters in Ankara and 293 in the provincial units. However, it is not possible to distinguish the level of expertise of the staff in the production of financial intelligence and/or if they only support operational needs in the field.
    b. TNP Narcotics oversees complex international investigations related to drug trafficking and the laundering of proceeds from this crime and plays a guiding and co-ordinating role in ML investigations conducted in Türkiye. Although they operate in the 81 provinces, approximately 30 officers are based in headquarters and 120 in the provinces. In addition, this department is supported by other TNP departments that conducts operations in the field in relation to ML and drug trafficking enforcement actions (i.e., control deliveries, search warrants, intelligence, etc) with approximately 3 100 officials supporting this work. In sum, a total of 3 250 officials is dedicated to ML and drug trafficking investigations, but only 5% are dedicated to the production of financial intelligence while the 95% supports operational needs in the field.
    c. Migrant Smuggling and Border Gates Department operates in the 81 provinces with 148 officials dedicate to ML investigations in headquarters and 151 in the remaining cities.

[31] Ankara, Antalya, Adana, Bakırköy, Bursa, Diyarbakır, Gaziantep, Istanbul, Istanbul Anatolia, Izmir, Kayseri, Konya, Küçükçekmece, Mersin and Şanlıurfa.

[32] Batı, Denizli, Eskişehir, Gebze, Karşıyaka, Kocaeli, Mardin, Sakarya, Van, Büyükçekmece.

   d. Cybercrime Department (TNP Cyber) oversees cybercrime investigations and the proceeds of this crime, particularly investigating illegal betting and cyber-enabled fraud. With a total of 3 198 officials, only 198 (6%) are engaged in ML investigations. However, it was not possible to assess their level of expertise on investigating ML.
   e. Public Security Department assigned 202 personnel in the Criminal Proceeds Bureau Commands in headquarter and provincial units.

b) The GGC organised crime unit (GGC KOM) has 1 404 officials dedicates to conduct ML investigations throughout the rural areas of the country. However, it was not possible to assess the type of support they can provide to public prosecutors.

c) The CGC and CE also have responsibilities in investigating ML offences. There are 2 700 officials from the Customs Protection Unit, and 200 officials from the Coast Guard Command but it was not feasible to determine how many of them are ML experts and contributes to supporting ML investigations, limiting their ability to detect and identify cross-border currency movement, high levels of smuggling, and transnational drug trafficking.

451. TNP supports most ML investigations (95%), the GGC only supports a limited number of ML investigations (5%) given their areas of competences as the GGC operates primarily in rural areas. This difference also explains the significant difference between TNP and GGC resources assigned to ML investigations. Both agencies have demonstrated their involvement in investigating large and complex ML cases and have shown strong co-operation when predicate offences occur across both rural and urban areas. In rural regions, ML investigations linked to fraud are primarily managed by the Gendarmerie KOM and the Proceeds of Crime Bureau, while in urban areas, responsibility lies with the TNP KOM. Prosecutors generally adhere to this division of expertise but may involve additional units or form joint investigation teams when needed, for instance, combining TNP KOM with TNP Cyber for cyber-related fraud cases. TNP demonstrates broad range effectiveness of financial investigation techniques to investigate complex case that misuse shell companies', VAs, PML and TBML. TNP also using digital forensic techniques to trace the asset through investigating social media and instant messaging, also conducting joint operation with multi-foreign counterparts (see IO.2) and requesting information to global VASPs. Other LEAs demonstrate limited extent effectiveness, particularly to investigate complex ML related to drug trafficking and smuggling which is not aligned with country's risk profile.

452. In addition, there is a limited need for participation of other LEAs when supporting ML investigations mainly due to the scope of their work and procedural mandates. For example, the CGC prevents crimes at sea and immediately informs the competent prosecutor once the case reaches land, enabling co-ordination with TNP or the GGC. However, given the risks of cross-border currency movement and high smuggling levels, as well as transnational drug trafficking, the limited number of investigations initiated by CE and their collaboration with prosecutors remains a concern.

Box 7.1. Trade-based ML investigation

Sunflower case

The investigation started upon a victim denunciation to the Chief Public Prosecutor's Office in province "A", which led to investigation for organised aggravated fraud and ML, with foreign links. The Public prosecutor was supported by TNP KOM during the investigation phase.

The investigation revealed that the criminal network was targeting businesspeople located in Middle East and European Countries under the guise of marketing sunflower seed oil to attract foreign investments. Although these companies had no registered activities, suspects working as customs brokers issued false documents and bills of lading. Even after the judicial investigation started, the organisation established a new company at the same address under a different name. The organisation's leader, S.Y., concealed the control of these companies by registering himself as a worker while remaining the true beneficial owner.

The laundering process was equally sophisticated: suspect B.A. converted funds into VAs through VASP and transferred them abroad to obscure the tracing of the proceeds, while others, like Y.K. and M.T., funnelled thousands of euros (approximately 4 100) through payment institutions to also obscure the tracing of assets. The fraud's proceeds moved through layers of FI accounts by company managers and where then transferred to third-party owned accounts. To then been transferred to jewellers' who purchase physical gold and luxury watches to integrate the illicit funds.

Results of the investigation

In 2023, simultaneous operations were launched in 5 provinces under the co-ordination of the Chief Prosecutor in province A, leading to the arrest of 49 suspects and the seizure of numerous physical and digital materials incorporated as evidence during the ongoing prosecution. A total of EUR 6 M is estimated to have been laundered by organisation, from which approximately EUR 2.5 M were seized along with 20 grams of gold, luxury brand watched, real state and luxury vehicles.

453. Prosecutors may also request information, documents, and expertise from other institutions to ensure comprehensive case handling. When conducting PFIs in complex ML cases, public prosecutors generally request MASAK to provide financial intelligence and analysis. Both LEAs and prosecutors have highlighted the quality and importance of MASAK's reports when targeting ML networks with international connections. In addition, when the complexity of the case requires it, FIU officials has been assigned to work jointly with LEAs in the financial analysis of an investigation. Although this demonstrates a solid co-ordination among Türkiye's operational authorities, including the robust request of financial intelligence and analysis to MASAK, this also indicates a more limited ability for LEAs to independently analyse financial information when conducting parallel financial investigations in relation to complex ML cases.

454. Türkiye investigate cases with foreign links to a large extent. However, its investigative capacity remains more limited in relation to complex ML activities involving professional, cross-border movements, particularly those associated with drug trafficking and smuggling. Due to the robust financial information collected by the competent authorities, in case the domestic criminal activity or assets are detected within Türkiye's borders, competent authorities use all investigations tools available to disrupt the ML activity and have demonstrated good results in disrupting organised crime structures operating in several jurisdictions.

Box 7.2. ML investigation triggered by a foreign predicate offence

Operation Comanchero.

Operation Comanchero, launched in November 2023, was a co-ordinated operation across eight cities, led by the TNP Counter Narcotics Department with support from city A Chief Public Prosecutor's Office, MASAK, and city A Police. The operation targeted the laundering of drug trafficking proceeds and involved high-profile suspects: nine individuals wanted internationally under INTERPOL Red Notices and another nine under Blue Notices. These suspects were linked to serious crimes, including drug trafficking, organised crime, money laundering, obstruction of justice, armed robbery, arson, and even murder. The criminal organisation was led by Mr. A, a double national (Turkish and Australian) who was listed in Australia's most-wanted list.

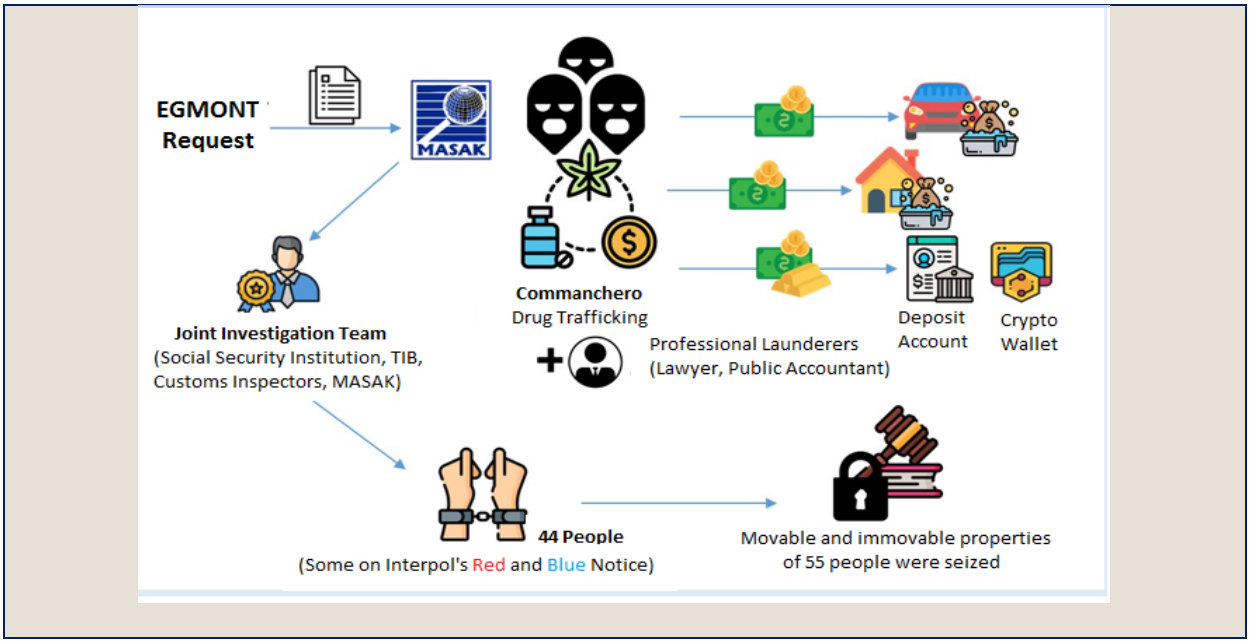
The ML investigation was triggered by open-source research initiated by MASAK (FIU) upon an EGMONT request on the links between the international motorcycle gang "Comanchero" and their business in Türkiye. The financial intelligence and analysis conducted by the FIU revealed that majority of proceeds from drug trafficking were deposited into the banking system as cash (in foreign currencies or as gold coins) and were used for purchasing properties and motor vehicles, transferred for funding shell companies or individuals. They also transferred funds through VASP. Moreover, some of the organisations where only involved in the provision of technical assistance in the laundering process as professional launderers (lawyer, financial consultant).

MASAK disseminated a financial analysis report (FAR) to city A Chief Public Prosecutor Office, city A Police and the TNP Counter Narcotics Department, including the financial profile of 55 individuals and 22 companies. To deepen the investigation, a Joint Investigation Team was established, comprising inspectors from the Social Security Agency, Tax Inspection Board, Customs, and FIU experts. Their mandate was to uncover links between suspects and companies, analyse digital evidence, and identify laundering activities. These efforts revealed a broader financial network, significantly expanding the scope of the investigation.

In parallel with the financial investigation, authorities uncovered strong connections to large-scale drug trafficking operations. Australian and Turkish judicial authorities held five co-ordination meetings, and a formal request was made to transfer the lawsuit related to the predicate offence tied to the Australian "Comanchero" operation. The information exchanges have been made with 25 countries, Evidence revealed that the criminal organisation, led by Mr. A, orchestrated the transport of drugs sourced from Türkiye and South America to destinations including Australia, the Netherlands, and Hong Kong, China, using transit routes through South Korea and South Africa. Between 2018- 2021, LEAs seized approximately 4 000 kilograms of narcotics—cocaine, methamphetamine, and ecstasy—linked to this network, underscoring the transnational scale and severity of the underlying criminal activity.

Results of the Investigation

Assets pertaining to 55 people including professional launderers and domestically or internationally wanted persons were seized and 44 people were arrested by the decision of city A 3rd Criminal Court of Peace. The prosecution is ongoing. i



455. Türkiye progressively incremented the number of ML investigations since its last MER in 2019. Between 2021-2025, Türkiye opened approximately 23 184 ML investigations, with a significant surge in 2024 (33%) and 2025 (43%). However, given Türkiye's contextual and material factors (i.e., size of the financial sector, geographical position as a transit hub, the extent of cash based, and size of informal economy), ML investigations, prosecutions, and convictions in high-risk areas other than fraud (i.e., professional, misuse of legal person, and cross-border movement) (see IO.1) is more limited.

456. Fraud (including aggravated fraud) is the most relevant predicate offences of ML with total 16 586 cases (80%), followed by a low number of investigation in other high and medium risk predicate offences, such as illegal betting with 1 428 (7%), drug trafficking with 1 267 cases (13%), customs smuggling with 590 cases (3%) which is not aligned with the country's risk profile.

Table 7.2. ML investigation files (2021-2025)*

Year	ML Files	Suspects	Offences charged
2021	514	2168	2595
2022	1585	5335	6541
2023	3469	8969	10662
2024	7700	14650	16601
2025**	9916	18531	22930
Total	**23184**	**49653**	**59329**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

457. Türkiye identifies different type of ML activity while conducting investigations, being self-laundering (48%) and third-party money laundering (35%) the most predominant ones in line with the country risk profile, including effective stand-alone ML related to illegal betting. However, the reviewed case studies demonstrate a limited extent of stand-alone ML investigations related to fraud and other predicate offences, notwithstanding the country's risk profile as a hub or destination for the transfer of proceeds of crime derived from foreign predicate offences.

Table 7.3. ML investigations disaggregated per type of ML offence (2021-2025)*

Year	Third-party ML	Self-laundering	Self-laundering and third-party ML	Foreign predicate offence	Total investigations/year
2021	856	1373	316	50	**2595**
2022	3060	2740	516	225	**6541**
2023	3865	5817	744	236	**10662**
2024	2973	3908	2504	72	**9457**
2025**	3554	5359	2558	67	**11538**
Total	**14308**	**19197**	**6638**	**650**	**40793**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

458. Türkiye demonstrates positive development on numerous complex ML and transnational cases, except ML activities that involve professional ML and cross-border currency movement, which resulted in numerous arrests, disruption of large networks. Notwithstanding the robust international co-operation, competent authorities face challenges to secure and recover assets located abroad (see IO.8). Despite these efforts, improvements in investigations involving cross border cash movement, unlicensed intermediaries (i.e., hawala, foreign exchanges), and misuse of legal persons that include facilitation by accounting and legal professionals are also needed. Although fraud, drug trafficking, and smuggling are assessed as high or medium-risk predicate offences, public prosecutors and LEAs face challenges in tracing crime proceeds due to limited understanding of complex laundering methods such as cash smuggling, professional money laundering networks, hawala, and foreign exchange operations. This gap is particularly significant given Türkiye's role as a transit hub for global financial flows (see IO.1).

7.2. Prosecuting and convicting different types of ML activity[33]

459. Türkiye extensively pursues prosecutions and recorded convictions related to all type of ML offences, except for stand-alone ML and ML derived from foreign predicate offences. The investigation-to-prosecution rate is about 46% which is commensurate with Türkiye's risk profile and context to some extent, as low initiation thresholds are required for investigations while proving the knowledge and intention for to pursue prosecutions and convictions remains more complex. The effectiveness of the implementation of the national strategy for investigating and prosecuting ML is evidenced by a 42-fold increase in the number of prosecutions between 2021 and 2025.

460. Between 2021 and 2025, Türkiye has prosecuted 10 581 cases for ML offences. Prosecutions are predominantly related to self-laundering (56%), third party ML (25%), a combination of both categories (18%). In addition, standalone ML prosecutions are only limited to illegal betting-related cases and has not been applied to other type of predicate offences. Türkiye achieved convictions in 556 cases, predominantly in self-laundering cases (55%) followed by third-party ML cases (26%) and a combination of both (19%), including effective stand-alone ML related to illegal betting. Given Türkiye's risk as transit hub for funds and destination to transfer proceed of crimes related to fraud and other predicate offences, the stand-alone ML prosecution and convictions is more limited. There are several case studies demonstrate the prosecution of foreign predicate offences triggered by domestic predicate offences or foreign elements

[33] *See Methodology, IO.7, Note to Assessors 2 and related footnotes*

within those and three cases of convictions related to independent foreign predicate offences. The table below provides a detailed explanation of these numbers including investigations.

Table 7.4. ML types of investigations, prosecutions and convictions (2021-2025)*

ML type	2021	2022	2023	2024	2025**	Total/ reporting period	%	Pending files
INVESTIGATIONS								
Self-laundering	1373	2740	5817	3908	5359	19197	47%	3286
3rd party ML	856	3060	3865	2973	3554	14308	35%	1989
Together (Self-laundering and 3rd party ML)	316	516	744	2504	2558	6638	17%	1856
Foreign predicate offences	50	225	236	72	67	650	2%	117
Total investigations	**2595**	**6541**	**10662**	**9457**	**11538**	**40793**	**100%**	**7248**
PROSECUTIONS								
Self-laundering	867	491	2017	1848	3159	8382	56%	3796
3rd party ML	378	395	1295	680	990	3738	25%	934
Together (Self-laundering and 3rd party ML)	195	115	263	811	1337	2721	18%	1301
Foreign predicate offences	9	31	9	31	16	96	1%	54
Total prosecutions	**1449**	**1032**	**3584**	**3370**	**5502**	**14937**	**100%**	**6085**
CONVICTIONS								
Self-laundering	38	87	85	76	186	472	55%	
3rd party ML	7	6	35	42	133	223	26%	
Together (Self-laundering and 3rd party ML)	16	25	21	28	69	159	19%	
Foreign predicate offences	0	0	0	1	2	3	0%	
Total convictions	**61**	**118**	**141**	**147**	**390**	**857**	**100%**	

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

461. Although ML prosecutions and convictions are in line with Türkiye's risk profile, particularly for fraud and illegal betting, this is not the case for medium-high risk and medium predicate offences (i.e., drug trafficking and smuggling). Prosecutors presented challenges in prosecuting complex ML schemes involving sophisticated layering structures, including legal persons, shell companies, misuse of legal professionals and trade-based mechanisms, and systemic layering networks, as well as the misuse of technology.

462. The data reveals that prosecutions still pending represents the 47% (7 248) of those already finalised (14 937), and the number of pending convictions (6 085 files) exceed finalised convictions (556) by a factor of nine. Authorities attribute the significant backlog of prosecutions to the complexity and scope of cases and the appeal which require extended timeframes for resolution. The absence of a clear guidance to prioritise ML prosecutions, combined with the average 1.5-year timeframe required to complete a single ML case, contributes to the accumulation of these cases generating significantly impacting the prosecutors and LEAs workload. Conviction rates are expected to rise gradually as these cases advance through the judicial process and reach the verdict stage.

463. In addition, it is important to note that the number of natural persons subject to investigations, prosecutions and being convicted varies considerably. The total number of natural persons convicted represents only the 2% of those subject to investigation which also implies challenges in attributing the criminal activity to the prosecuted person at a conviction stage. In these regard, competent authorities signalled challenges in proving knowledge and intention during trial.

Table 7.5. Natural persons subject to ML investigations, prosecutions and convictions (2021-2025)*

Criminal procedure stage	2021	2021	2023	2024	2025**	Total
Suspects subject to investigation	2168	5335	8969	14650	18531	**49653**
Defendants subject to prosecutions	1421	976	2902	6409	10374	**22082**
Convicted persons	61	116	137	253	391	**958**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

7.3. Effectiveness, proportionality and dissuasiveness of sanctions

464. Türkiye applies average 4-years 4 months imprisonment for natural persons convicted with ML charges which is considered effective, proportionate, and dissuasive in general. However, the low application of criminal sanctions on complex ML cases, including the involvement of professional money launderers, and in those related to organised crime undermines the overall dissuasiveness of the sanction framework.

Table 7.6. Sentences applied to natural persons for ML offences (2020-2025)

Type of sentence	2020	2021	2022	2023	2024	2025*	Total	Ratio on type of sentences applied
Fines only	5	-	1	25	4	4	**39**	4%
0-3 years of imprisonment	16	26	27	61	143	321	**594**	58%
>3- 5 years of imprisonment	11	22	22	21	92	47	**215**	21%
>5-10 years of imprisonment	29	2	61	29	14	13	**148**	15%
>10 years of imprisonment	-	11	5	2	-	6	**24**	2%

Note: (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

465. In accordance with the principle of personal liability for criminal penalties, Türkiye cannot apply criminal sanctions to legal persons, but is able to apply administrative sanctions (i.e., confiscation measures, appointment of receivers, license revocation or cancellation, fines, among others). Türkiye has demonstrated the application of administrative sanctions (14 receivers' appointments, 6 licenses revocation or cancellation, and 13 seizure measures) to 18 legal persons, such as, payment institutions, a bank, a VASP, a licensed betting platform and a media company through case studies. Although this demonstrates Türkiye's ability to implement sanctions to legal persons, the number of sanctions applied is neither dissuasive nor commensurate with the country risk profile given the increasing use of professional money launderers, the multi-layered ML schemes, including through the creation of shell companies, cargo and logistics companies, and exchange offices facilitating ML activities (see IO.1). The lack of clear and systemic implementation of administrative sanctions and fines to legal persons negatively affects the effectiveness and dissuasiveness of the sanctions.

7.4. Use of alternative measures

466. Türkiye applies alternative measures when securing a ML conviction is not feasible, provided evidentiary standards are met (e.g., pursuing tax evasion or other predicate offences).

467. When it is not possible to reach a ML conviction, Türkiye applies laundering of stolen goods charges (art. 165) to secure a conviction and tax evasion charges. Article 165 serves as a practical mechanism to criminalise laundering activities, applying a "probable cause" evidentiary standard. Under this provision, individuals can face criminal penalties for simply selling, transferring, purchasing, or accepting criminal property without the need to prove specific intent. Between 2021 and 2025, 23 266 convictions were secured under Article 165.

468. Türkiye also employs tax evasion measures as an alternative measure and presented a case example where this was applied in the context of forged documents. However, despite initiating over 220 664 investigations and 146 808 prosecutions for tax evasion between 2020 and 2025, resulting in approximately 91 285 convictions, authorities have not demonstrated how these cases function as an alternative for ML convictions.

8 Asset recovery

The relevant Immediate Outcomes considered and assessed in this chapter is IO.8. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 32 and elements of R. 15, 30, 31, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Türkiye prioritises asset recovery as a national and operational policy objective at the highest level. Asset recovery policies are reviewed periodically through the Threat WG considering the operational findings, trends and international experiences which guarantees an up-to-date asset recovery system.

b) These policies have translated into enforcement actions progressively and competent authorities identify and trace criminal property and property of corresponding value domestically to a large extent. However, there is limited evidence of effective tools or measures to identify and trace assets located abroad representing a major shortcoming in the overall asset tracing mechanism. Significant data limitations and the very low contribution of financial intelligence to asset identification, undermine the authorities' ability to comprehensively identify and trace assets, particularly in cross border investigations.

c) Türkiye has a well-developed framework to measure the assets of corresponding value. For simple cases, the LEAs executing the seizure declares value of the asset and report it to the public prosecutor, while in complex cases judges can assign specialised experts witnesses to measure the value of assets.

d) MASAK have applied postponed transactions in 19 276 files resulting in the freezing of more than EUR 1 138 M until verification of the legitimacy of the transaction (7 working days). However, only 3.2% of those files resulted in seizures.

e) Türkiye has made measurable progress in the use of asset recovery tools. Türkiye seized assets for EUR 147 M and confiscated EUR 93 M. Half of these assets were seized and confiscated in 2024-2025, indicating a positive response to the implementation of new strategies and policies on asset recovery. Despite these positive trends, the overall conversion of provisional measures into seizures and confiscations remains limited given Türkiye's risk profile. In addition, the operational framework does not allow for a clear distinction between those assets seized or confiscated as criminal property or as property of corresponding value.

f) LEAs and prosecutors have demonstrated some positive results to seize and confiscate assets through different ML/TF case studies, even in multijurisdictional investigations. However, assets repatriation and international enforcement mechanisms are applied to a limited extent.

g) Türkiye has different mechanisms in place to manage, and dispose seized and confiscated property with the aim of preserving its value. VAs management system was recently updated (June 2025) given the currency volatile nature, demonstrating Türkiye's quick response to address operational challenges in the asset recovery system. However, insufficient information prevented an assessment of the overall effectiveness of asset value preservation mechanisms.

h) Türkiye has a solid legal framework for cross-border cash declaration and disclosures coupled with high-level technology to detect illegal movements of cash in all land and air check points. Despite these efforts, the number of non-declared or falsely declared cross-border currency and BNI movements detection and seizure remains limited. This is not aligned with the country's risk profile as customs-smuggling is rated as a medium risk in the 2025 NRA. The limited number of cross-border seizure of cash (1%), weapons or ammunition (1%), fuel and other petroleum products (1%) is concerning given Türkiye's risk and context. In addition, it is not possible to conclude how many of these assets were subject to final confiscation.

Key Recommended Actions (KRAs)

Türkiye should:

p) Strengthen its capacity to identify, trace and recover criminal assets located abroad, particularly in complex and cross-border criminal asset recovery cases. This requires both enhanced inter-agency co-ordination domestically and more systemic and timely use of international co-operation tools, including making a better use of Mutual Legal Assistance requests to recover these assets.

q) Strengthen cash controls effectiveness in customs supervised areas prioritising enhanced screening for inbound cash movements, including improved data analytics to identify high-risk patterns, increased co-ordination between Customs Enforcement, other LEAs and MASAK to ensure that declarations translate into enforcement outcomes.

Other Recommended Actions

a) Enhance the use of operational application of post-conviction and non-conviction-based confiscations mechanisms, including through guidance and trainings.

Overall Conclusions on IO.8

Türkiye places asset recovery as a top national and operational priority, supported by well-developed legal and institutional frameworks. Legislative measures are progressively producing positive results, with policies regularly updated and sufficient resources allocated to trace and identify criminal property and property of corresponding value domestically. This demonstrates Türkiye's strong and evolving commitment to recover proceeds of crime. However, several challenges are still identified when identifying, tracing and enforcing confiscation orders of assets located abroad representing a major shortcoming in the overall asset confiscation and repatriation mechanism process given Türkiye's risk profile.

Türkiye has made measurable but modest progress in the use or asset recovery measures. Competent authorities implement a provisional measure (named postponement of transaction) to a very large extent at an administrative level and with the aim of verifying the legitimacy of the transactions. While seizure and confiscation are applied in the context of a criminal investigation and to a lesser extent. The overall conversion from provisional measures to actual seizures and confiscations also remains limited. Türkiye's total number of assets seized (EUR 147 M) and confiscated (EUR 93 M) is modest given its risk and context, these results are largely driven by high-value complex cases mainly triggered by international co-operation requests. In addition, it is not possible to distinguish the percentage of seized and confiscated assets representing criminal property from those representing assets of corresponding value.

Türkiye operates a hybrid system for addressing undeclared or falsely declared cross-border currency movements. Despite significant investment in advanced technology at Customs Enforcement checkpoints, detections and seizures of such movements remain limited, which is inconsistent with the medium cash-smuggling risk identified in the 2025 NRA. The disparity between incoming cash declarations (EUR 87.9 billion vs. EUR 25.4 billion outbound), along with disclosed amounts (EUR 435 M inbound vs. EUR 77 M outbound) combined with minimal seizures (506 files), highlights weaknesses in current controls. Furthermore, Customs Enforcement limited dissemination of only 463 reports to LEAs and MASAK for further analysis, suggests enforcement and risk management gaps at entry points. These factors collectively indicate limited effectiveness in mitigating cross-border cash-smuggling risks.

Türkiye is rated as having a Moderate level of effectiveness for IO.8.

Immediate Outcome 8

8.1. Prioritisation of asset recovery as a policy objective and using effective agency structures and co-operation frameworks

Prioritising asset recovery as a policy objective

469. Türkiye prioritises asset recovery as a national and operational policy objective at the highest level including through its Judicial Reform Strategy Document (updated in 2025), the Strategy Document for Increasing Effectiveness in AML/CFT and Confiscation Practices (2021-2025), and operational documents and guidelines produced by competent authorities in the context of their duties (for example, the FIU regarding confiscation of VAs).

470. The Judicial Strategy Document is the highest policy document on judicial matters including criminal policies related to asset recovery. Under its Strategic Objective 3 titled *"Increasing the Effectiveness of the Criminal Justice System"* Türkiye aims at making the necessary arrangements to: (i) solve problems arising from confiscation and seizure in criminal proceedings; (ii) enhance the identification, confiscation and management of the proceeds of crime; and (iii) establish an institutional structure for the purpose of improving Türkiye's asset recovery systems by examining international examples. The document also includes objectives to strengthen judicial authorities' human resources and capacities to improve the asset recovery system.

471. Following the guidance in the Judicial Strategy Document, the FIU prepared and published the Strategy Document for Increasing Effectiveness in AML/CFT and Confiscation Practices for the 2021-2025 period emphasising the need for depriving criminals of their proceeds and enhancing financial intelligence capabilities for the implementation of effective seizure and confiscation measures in ML, associate predicate offences, and TF. The implementation of the Strategy is supported by three working groups and sub-groups at a national level which includes all competent authorities relevant to the asset recovery process.

472. As part of its ICRG action plan and beyond, Türkiye has also introduced a performance-based approach to asset recovery, aiming to ensure accountability and institutional efficiency in the implementation of seizure and confiscation measures. To this end, a series of specific, measurable criteria have been established across relevant institutions to clarify mandates and monitor effectiveness in recovering the proceeds of crime. Türkiye's judicial performance evaluation framework has integrated asset recovery expectations into the core duties of judges and prosecutors. Specifically, it requires public prosecutors to initiate parallel financial investigations in ML/TF cases, apply seizure and confiscation orders proactively, and consider proportional restraint measures to prevent asset dissipation. Integrating asset recovery into performance evaluation mechanisms helps ensure that institutional priorities are internalised at the individual level. By tying prosecutorial and judicial advancement to the effective use of financial investigative tools and confiscation measure. Türkiye fosters a results-oriented culture that reinforces the broader policy objective of depriving proceeds of crime. As a result of the implementation of the performance evaluation over the past two years, forty-seven specialised ML/TF public prosecutors were not promoted because they did not fully meet the performance criteria described above demonstrating the effective application of the system.

473. In addition, the MoJ Circular No. 155/1 prioritises conducting PFIs in line with national risks as part of Türkiye's broader criminal policy and increasing the effectiveness of implementing seizure and confiscation processes, effectively enforce security measures and administrative sanctions for legal entities in cases of ML/TF and ensure specialisation in conducting investigations. This circular is applicable to all public prosecutors and courts in the 81 provinces and is operationally oriented, providing competent authorities with the procedures for the seizure and confiscation of property and funds. Public prosecutors should in all cases:

a) Conduct a detailed examination of bank loans, bank and traveller's checks, remittances, transfers, securities, stocks, VAs, guarantees, bonds, bills, policies, letters of credit and similar assets that can be represented by money or money value, and all kinds of movable or immovable, tangible or intangible, all kinds of goods, rights, receivables and all kinds of economic values, including those in electronic or digital media that certify and represent a property right or interest on them, and determine the assets of persons in close relationship with the suspect;
b) Examine whether assets were taken abroad and explore ways to trace them.
c) Apply all effective investigative techniques.
d) Consider seizure and confiscation of assets at early stages of the prosecution when preparing indictments for ML/TF offences.

e) Examining the funding issue separately in the investigations conducted to those suspected of being founder or leadership of a terrorist organisation for TF cases.

474. The practical orientation of the Circular helps to translate national policy goals into day-to-day operational guidance. By providing structured expectations across all provinces and reinforcing them through regular evaluation meetings, the system supports a more coherent and results-driven approach to asset recovery.

475. The MoI also issued a circular to strengthen LEAs practices in effectively combating offences that generate proceeds of crime and ensuring the identification and deprivation of such assets for the benefit of the State. LEAs should:

a) Conduct comprehensive financial profiling and asset-tracing activities covering immovables, vehicles, bank accounts, receivables, negotiable instruments, company shares, and other tangible or intangible assets.
b) Gather financial intelligence from relevant institutions, particularly MASAK, to support the identification of criminal proceeds and related actors.
c) Perform parallel or integrated financial investigations in cases involving predicate offences with potential proceeds, especially those assessed as high or medium risk in the NRA.
d) Secure timely seizure of suspected proceeds of crime, ensuring these measures are taken under the legal framework and promptly submitted for judicial approval, as per the CPL and the AML Law.
e) Include detailed information in the case file regarding the origin, nature, and estimated value of the assets, including documentation to support confiscation decisions.
f) Differentiate assets whose criminal origin cannot be definitively proven to facilitate value-based confiscation and expose potential concealment schemes.
g) Refer assets at risk of damage or loss of value for judicial authorisation of pre-conviction disposal to protect both public interest and third-party rights.
h) Record the appraised value of seized assets in the national enforcement system (EKIP) and ensure all actions are lawfully executed.

476. The MoI circular also considers asset recovery as a strategic priority and instructs field units in all 81 provinces to act in co-ordination with PPOs. It mandates timely reporting, cross-institutional co-operation, and adherence to procedural safeguards to ensure the legality and effectiveness of all seizure and confiscation measures.

477. The policies implemented to strengthen asset recovery system in Türkiye have progressively translated into tangible operational results. The MoF and MASAK's internal frameworks have enhanced the systematic use of postponement of transactions, ensuring that freezing measures are applied periodically and effectively following financial analysis. Likewise, the MoJ circulars have reinforced the prioritisation of seizure and confiscation within criminal proceedings, enabling prosecutors and judges to apply these mechanisms more consistently. Overall, these measures demonstrate a clear prioritisation of asset recovery as a policy objective which is positively translating into the operationalisation of asset recovery tools.

8.1.1. Periodic review of asset recovery regime

478. Türkiye demonstrates a robust history of prioritising asset recovery as a policy objective which is complemented by the periodic revision of the legal framework and practices, considering emerging risks, evolving typologies, and international standards. Türkiye's CBCFC is the competent authority for reviewing the asset recovery regime. Within the CBCFC, the MoJ leads the drafting process for amending policies and legislation and designing new ones, which are then discussed with all relevant authorities, including MASAK, LEAs and PPOs, through the CBCFC Threat Working Group. These multi-agency efforts ensure that

asset recovery practices are not static but subject to ongoing review and adjustment. Through annual evaluations, regular data collection, and co-ordinated feedback mechanisms, Türkiye maintains a responsive and evolving confiscation regime that reflects operational realities.

479. As a result of these co-ordination mechanisms, the Judicial Reform Strategy Document (enforced in 2009) was reviewed and followed by strategy documents in 2015 and 2019. Since 2021, the Threats and Vulnerabilities WG hosted twenty-five meetings to discuss amendments to the asset recovery regime resulting in: (i) a full update of the Judicial Reform Strategy Document (covering the years 2025-2029); (ii) the publication of FIU's Strategy Document for Increasing Effectiveness in AML/CFT and Confiscation Practices for the 2021-2025 period; (iii) adoption of the MoJ Circular 155/1 which resulted in periodic evaluation meetings held by the Directorate General for Criminal Affairs and the PPOs with the objective of keeping the asset recovery system up to date and enhance seizure and confiscation procedures.

480. The period for revision of these documents is not stated in the legislation. However, competent authorities have demonstrated to routinely review them through the above-mentioned mechanisms.

8.1.2. Effective agency structures and co-operation frameworks

481. The CBCFC plays a central role in ensuring co-operation and co-ordination among all AML/CFT relevant competent authorities including in the development of strategies and mechanisms to enhance the effectiveness of asset recovery efforts, reviewing draft legislation and strengthening interagency co-operation when implementing asset recovery strategies. The CBCFC is chaired by the MoTF and integrated by policy and operational AML/CFT authorities at the highest level (Deputy Director of the National Intelligence Organisation, General Director of Financial Markets and Foreign Exchange, Head of the Tax Inspection Board, Head of the Financial Crimes Investigation Board, MoJ Director General of Criminal Affairs, MFA Director General of Intelligence and Security, MoT Director General of Customs Enforcement, BRSA Deputy Chairman and the TNP Deputy director General) which demonstrates Türkiye's integral approach to the development of asset recovery criminal policies. Most of legislations revisions were conducted between 2023-2025 and their implementation have recently started to show positive results with an increment of 50% of FIU's financial reports on proceeds of crimes in 2024, over 75% of postponement of transactions and 90% of files subject to seizure and confiscation issued between 2023-2025.

482. This interagency co-operation approach is also translated into operational levels through the implementation of asset recovery criminal policies in investigations and prosecutions. In all stages of ML/TF investigations and prosecutions, competent authorities are required to register all information related to the proceeds of crimes and their status (seized or confiscated) in the UYAP which facilitates operational authorities searches all kinds of data (such as amount, quantity, type, value, etc.) and documents of assets taken under custody, seized or confiscated, enhancing the co-ordination mechanisms between prosecutors, LEAs and authorities managing the seized and confiscated assets, including tax authorities.

483. Operational findings and contribution of LEAs (TNP, GGC and CE) and MASAK are also regularly informed to the MoJ with the aim of keeping these frameworks up to date in alliance to the operational trends. This allows a continuous assessment and supports a more responsive and impactful regime flexible enough to adapt to the changing nature of criminal threats providing effective and timely responses to prevent the dissipation of illegal proceeds of crimes.

8.2. Identifying and tracing criminal property and property of corresponding value

484. Türkiye demonstrates a good number of resources to prioritise asset recovery at an operational level and can identify and trace criminal property domestically to a large extent. However, no information was provided on tools used to identify and trace assets located abroad. Considering Türkiye's risk and context profile, characterised by a significant trade activity, substantial foreign investments, exposure to smuggling risks and the presence of cross-border criminal organisations, the limited ability to identify and trace assets located abroad represents a major shortcoming that constraints the overall effectives of the country's asset recovery system.

485. Prosecutors and LEAs have mechanisms in place to identify and trace criminal property and property of corresponding value, whether located domestically or abroad (see R.31) and regularly do so for assets located domestically. Public prosecutors often request MASAK to identify and trace assets in the context of criminal investigations. Upon request, MASAK produces a financial analysis report identifying all assets linked to the suspects and refers it to the public prosecutor for decision on seizure or confiscation. Public prosecutors have highlighted the utility of these reports as positive.

486. The main responsibility for the identification and tracing of criminal property and property of corresponding value falls on Türkiye's Prosecutors and LEAs, who use different tools to collect evidence and, when possible, seize assets, including direct access to databases of the TRA, the General Directorate of Land Registry and Cadastre and the MoT and the UYAP system which allows them to conduct quick searches on the assets ownership of all suspects subject to investigations. In addition, the UYAP system also interconnects all available assets-related data in ongoing criminal investigations which provides prosecutors and LEAs with a robust roster of financial information for asset identification. Through these systems, competent authorities can identify bank account records, movable and immovable registries, tax records and shareholders information, among others. If needed, prosecutors can request other competent authorities (MASAK, BRSA, CMB, MoTF and the Accounting and Auditing Standards Authority) to identify new data either through their internal data bases or by international co-operation mechanisms (see IO.2).

487. Between 2024-2025, Türkiye identified 525 416 assets as criminal property or property of corresponding value in the context of criminal investigations, from which 1 197 were identified through MASAK's financial intelligence (0.23%) for seizure or confiscation purposes. However, no information was provided on the remaining years of the reporting period nor was the assessment team able to distinguish which of the assets belongs to each category.

488. Competent authorities use different methods to identify and trace criminal property and property of corresponding value. When conducting a PFI, authorities conduct a comprehensive review of suspects' assets to verify consistency with their legitimate income and activities. This includes examining movable and immovable property, bank and VAs accounts, and transactions involving close family members. Public prosecutors assess whether assets are disproportionate to income, trace their sources, and analyse the links of those assets to the criminal activity under investigation. In addition, they collect traditional physical evidence such as diaries, invoices, receipts, and bank cards are also seized when conducting search warrants to identify hidden accounts or third-party involvement. Additionally, social media activity and personal networks are scrutinised for connections to crimes.

489. Public prosecutors and LEAs also make the appropriate consultations through UYAP, searching for all kind of financial data available in Türkiye's system. For instance, all personal and financial data can be accessed through UYAP including the information of seized or confiscated assets valuations. As the determination of the value of seized immovable property, vehicles and valuables, as well as companies, requires specific expertise, it takes time to determine the value of many assets seized within the scope of the same investigation and to enter the data. For this reason, it is considered that the seizures and

confiscated figures seen in UYAP do not fully correspond to the actual situation and that this discrepancy will be resolved as the data entries are completed in the future.

490. Türkiye identifies property of corresponding value in cases where the assets or material benefits subject to confiscation cannot be seized or delivered to the competent authority, the equivalent value of such property can be confiscated. Upon the prosecutor's petition, the judge will examine the suspects' financial information and request a valuation expert (called expert witness) from the MoJ-approved list to determine the value of the asset potentially subject to seizure/confiscation. These experts are categorised by field of expertise (i.e., vehicles, real state, companies, etc.) and vetted by the MoJ Appraisal Department before integrating the list. Judicial authorities may directly assign experts by selecting the necessary areas of expertise from the expert witness search screen in UYAP. In complex cases, the judge can request expert witnesses to work in panels. For reporting purposes, they are required to fill out a form (jointly if being elaborated by a panel) with a checklist to specify the valuation of the assets. Although the competent authorities note the added value of expert witnesses in supporting the identification of property of corresponding value, the information provided offers limited insight into how these reports contributed in practice, including the extent to which they have resulted in the seizure or confiscation of assets of corresponding value.

491. This system is used throughout the country and there is a total of 36 235 experts witness registered in the 17 Experts Witness Committees to assist in the valuation process. Currently, the expert witness system comprises a total of 721 sub areas, including 63 core areas of expertise such as mining, archaeology, art and collectibles, ancient manuscripts and documents, cultural productions, media and communication. In order to ensure that reports are of a higher quality and standard, the Department for Expert Witnesses has established a common basic template for expert witness reports and expert witnesses are monitored to ensure that they fulfil their duties from the moment they receive the file for examination until its delivery.

492. The assigned expert witness or panel of expert witnesses prepares a report using their scientific and technical expertise in the case file they have examined. This report must be technically standard and meet the technical requirements requested by the prosecutor, judge or court. After conducting their research and examination within the previously specified timeframe, they fill out the standard form and submit it via UYAP and, if requested, also physically. The prosecutor or court can view the expert witness report simultaneously via UYAP. A copy of the final decision concerning the confiscation of their corresponding value shall be sent directly by the court to the chief revenue officer of the location where the decision was rendered.

493. Although Türkiye has a robust legal and institutional framework to identify property of corresponding value, only information on how witness experts contribute to assigning value to the asset was provided. The lack of information on its implementation and how many assets of corresponding value were seized and confiscated confirms the incipient implementation of the mechanism and prevents the effectiveness assessment.

8.3. Freezing and/or seizing criminal property and property of corresponding value Freezing and/or seizing criminal property and property of corresponding value

494. When a ML/TF or associated predicate offence are suspected, the MoTF has the authority to postpone transactions for seven working days (renewable), which allows MASAK to conduct the preliminary analysis to verify the suspicion, analyse the transaction, and if necessary, disseminate it to the competent authorities for seizing purposes. Türkiye considers the postponement of transactions as a provisional

measure equivalent to freezing of assets mechanism, covering a wide range of financial activities, including VASPs. Between 2021-2025, Türkiye has postponed transactions worth approximately EUR 1 138 M.

495. Within the seven days of verification, MASAK analyses all the financial information related to the persons- natural or legal- executing the transactions (originator and beneficiary), the relevant indicators of the transaction (i.e., channel used, country of origin and destination) and all related financial information. Out of 19 276 postponements of transactions, only 612 (3.2%) resulted in asset seizure. The extremely low conversion rate suggests either an excessive reliance on the postponement tool or significant shortcomings in the judicial process for authorising seizures. Although a direct comparison between these figures can represent methodological limitations, as the total number of postponed transactions may include repetitive renewals of the same operation, the conclusion is reinforced by the absence of disaggregated data across the years limits the authorities' ability to clearly demonstrate the real ratio of postponement of transactions resulting in actual seizures or confiscations.

Table 8.1. Number of postpones transactions by MASAK resulting in confiscation (2021-2025)*

Year	Number of postponed transactions (PT)	Number of assets subject to postponed transactions (EUR)***	Number of confiscations	Amount confiscated (EUR)
2021	4663	€ 296,444,124.00	-	
2022	2111	€ 169,137,215.00	12	€ 56,196.00
2023	3091	€ 146,908,202.00	3	€ 60,221.00
2024	4635	€ 216,053,836.00	4	€ 237,978.00
2025**	4776	€ 309,385,966.00	9	€ 1,631,097.00
Total	**19276**	**€ 1,137,929,343.00**	**28**	**€ 1,985,492.00**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025). (***) Conversion rates were calculated on annual average bases as follows: year 2020 (1 TRY=0.12 EUR); year 2021 (1 TRY= 0.097 EUR); year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); year 2024 (1 TRY= 0.028); and year 2025 (1 TRY= 0.022 EUR).

496. Although Türkiye does not have in place other freezing mechanisms apart from the postponement of transactions and those related to the implementation of targeted financial sanctions (see IO.10), the implementation of postponement of transactions have led to seizure of assets and confiscation in some cases. For example:

Box 8.1. MASAK financial detection report leads to the seizure of EUR 28 000

An STR was submitted requesting the suspension of a transaction after wallet addresses linked to him were reported as being used to transfer illegal betting proceeds. Acting on strong suspicion of ML, MASAK applied a suspension of approximately EUR 28 000. MASAK prepared a financial detection report and disseminated it to the PPOs with a seizure request. After 15 days, the public prosecutor obtained a seizure order from the Criminal Court of Peace. The public prosecutor filled an indictment requesting the confiscation of assets seven months later.

Source: MASAK

497. Asset seizures are conducted in the context of a criminal investigation, and the seizure order must be issued by a judge. As the lead of investigations and prosecutions, public prosecutor instructs the relevant LEAs unit to identify and trace the property linked to the offence under investigation. Where delay is prejudicial, the public prosecutor is authorised to order the seizure directly in ML/TF cases. This decision must then be submitted to the competent judge for homologation within twenty-four hours. When

immediate action is required in urgent situations, LEAs can also seize property and instrumentalities exceptionally upon a written order of the head of unit. For example, when LEAs are conducting enforcement measures (i.e., search warrants, wiretapping, etc.) and physical evidence is found on illicit proceeds of funds, they can verbally report it to the public prosecutor to secure the evidence in urgent circumstances. For this purpose, a public prosecutor is appointed for emergency calls taking 24 hours turns. The public prosecutor will then initiate the formal seizure request order to prevent the assets for being transferred and will report the seizure decision to the judge within twenty-four hours. The judge is required to decide within forty-eight hours, otherwise, the seizure shall be deemed void.

498. Following Türkiye's asset recovery strategy, public prosecutors and LEAS have progressively included asset identification and tracing as part as their investigations strategies resulting in more request for seizure of assets during 2024-2025 (see table 8.1). LEAs do have strong co-operation and co-ordination with prosecutor as meetings prior to judicial investigations are being initiated to ensure documentation and verification of information prior proceeding to court. LEAs and prosecutors have presented a number of examples where this interagency co-operation have resulted in the detection and immediate seizure of assets.

499. At the end of an investigation, the prosecutor will request the asset confiscation to the trial judge in case there is reasonable grounds to understand that the proceeds of crime and/or assets were used or are a result of the offence under investigation. If the court finds the defendant guilty, the sanction applied will include both, the relevant sanction and the asset confiscation. If the defendant dies during the trial, proceedings continue, and the court may still order confiscation of crime proceeds and any property whose possession is inherently unlawful. Once the confiscation decision becomes final, the court forwards it to the Ministry of Treasury and Finance for enforcement, which then handles the liquidation process according to the asset type, without further court involvement.

500. Between 2021 and 2025, Türkiye has progressively implemented all available asset recovery tools. However, out of all the assets subject to these measures only the 13% are subject to seizures and 8.2% to confiscation which is not aligned with the country's risk profile. This low conversion rate from provisional measures to seizure and confiscation points to deficiencies at the criminal stage of asset recovery, linked to lengthy and complex procedures required to identify assets and secure their confiscation through the court. In addition, competent authorities are not able to distinguish whether if the assets subject to any of these measures are related to criminal property or property of corresponding value, which further limits the assessment on the extent to which asset recovery measures target all type of illicit proceeds in the context of a criminal investigation. See the table below:

Table 8.2. Total assets subject to postponement of transaction, seizure and confiscation (2021-2025)*

Year	Postponement of transactions (EUR) (***)	Seizure of assets (EUR)	Confiscation of assets (EUR)
2021	€ 296,444,124.00	€ 43,848,005.00	€ 31,177,633.00
2022	€ 169,137,215.00	€ 23,106,615.00	€ 6,133,628.00
2023	€ 146,908,202.00	€ 33,203,734.00	€ 14,558,166.00
2024	€ 216,053,836.00	€ 41,543,149.00	€ 36,226,217.00
2025**	€ 309,385,966.00	€ 5,863,040.00	€ 5,154,835.00
Total	**€ 1,137,929,344.00**	**€ 147,564,543.00**	**€ 93,250,477.00**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025); (***) Conversion rates were calculated on annual average bases as follows: year 2020 (1 TRY=0.12 EUR); year 2021 (1 TRY= 0.097 EUR); year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); year 2024 (1 TRY= 0.028); and year 2025 (1 TRY= 0.022 EUR).

501. Finally, Türkiye can seize and confiscate different type of other assets as part of criminal procedures. Between 2021-2025 Türkiye has seized a total of 921 assets and confiscated 560 which is not in line with the country's risk profile. Particularly in the number of bank accounts and immovable property being seized and confiscated.

Table 8.3. Type of assets subject to seizure and confiscation (2021-2025)

Type of asset	Number of seizures	Number of confiscations
Vehicles (land, sea or air vehicles)	322	203
Bank/FIs accounts	137	69
Negotiable instruments	21	8
Balance on safe deposits box	1	1
Partnership shares	5	3
Immovable property	111	69
Other assets	320	206
All kind of rights and claim	4	1
Total	**921**	**560**

8.3.1. Active pursuit of provisional measures resulting from financial investigations

502. Türkiye can implement these provisional measures as result of parallel financial investigations. For example, competent authorities successfully dismantled four international criminal organisations and seized a wide range of assets, including 1575 properties, 43 cars, 1765 bank accounts, 101 kg gold, EUR 1.7 billion, among others. These actions demonstrate their capacity to disrupt ML and organised crime networks by including the seizure of assets as part of the parallel financial investigation's strategies.

503. If deemed necessary, public prosecutors can request the MASAK to conduct financial analysis on specific cases to enrich the results of parallel financial investigations. In this context, the MoTF can apply can issue an order of postponement of transactions for MASAK to analyse the case-related transactions in a period of 7 working days (renewable). During this period, MASAK will determine if other measures such as freezing or seizing of assets should apply and report back to the public prosecutor. The large implementation of postponement of transactions (EUR 1 138 M) demonstrates Türkiye's ability to disrupt the movement or use of illicit assets before they can be further layered or integrated into the financial system. However, as explained above, the rate of these transactions leading to seizure remains very limited.

504. Türkiye applies specific measures for smuggled goods that are seized or detained at customs due to violations of customs regulations or anti-smuggling laws, demonstrating an ascendent trend in the confiscation of goods at customs supervised areas. The DGCE leads the seizure process at CE checkpoints. Between 2021 and 2025, they seized a total of nearly EUR 3.5 billion in customs check points, represented in vehicles (8%), miscellaneous items (20%), textile products (10%), Electronics (8.4%), precious metals (30.8%), among others. Although the total number of seizures may seem aligned with the country's risk profile, the limited number of cross-border seizure of cash (1%), weapons or ammunition (1%), fuel and other petroleum products (1%) is concerning given Türkiye's risk and context. The final confiscation of these goods or their return to the rightful owner is determined by a court decision at the end of the prosecution process. The lack of information on how many seized goods and assets ended confiscated limits the assessment on the extent to which asset recovery measures target all type of illicit proceeds in the context of a criminal investigation.

8.4. Managing frozen or seized property to preserve its value

505. Türkiye has mechanisms in place to manage and dispose of frozen and seized property. However, it was not possible to assess the effectiveness of these mechanisms in relation to the assets value preservation due to lack of information provided on this specific aspect though Türkiye has several measures that authorities have to apply to preserve value, such as sale of assets and using interest bearing accounts as explained below.

506. The procedures concerning the criminal properties are carried out by the Depository Bureau under the surveillance and control of the Chief PPO. Depository Bureaus are available in the 81 provinces. Immovable properties resulting in seizures are registered in the UYAP system under the name of the Public Treasury by the General Directorate of National Property (GDNP). In the case of movable assets, the judicial authority conducting the investigation (public prosecutor or LEAs) ensures the safe storage and inventory of items seized. Once released from judicial custody, these items are received, stored, and classified by the GDNP. Depending on the type of asset, appropriate actions such as storage, destruction, allocation to a public institution, or liquidation can be taken. When the administration of seized immovable, rights, and credits is necessary, a receiver may be appointed for the administration of these assets.

507. Türkiye applies different strategies to manage seized assets depending on the type of assets:

a) Receivers' appointments: these applies to the administration of seized immovable, rights, credits and companies. The judge instructs the receiver to preserve the asset value in accordance with the practices and standards observed by a prudent trader, up to five years, safeguarding its integrity and market value.
    a. For seizure companies in ML/TF cases, assets are managed under the supervision of Savings Deposit Insurance Fund (SDIF). The receiver will administrate the company to preserve its legitimate business. If the company's financial situation, partnership structure or market conditions requires, the receiver can request the sale of the company (totally or partially), its assets, or the companies' liquidation. Sale and liquidation procedures are carried out by the relevant company's board of directors/managers or receivers or the SDIF. The consent of minority shareholders is not required for sale and liquidation proceedings. After the debts have been paid at the end of the dissolution and liquidation proceedings, the remaining amount shall be held in an account bearing interest until the proceedings are finally concluded. Once the case reaches to conviction and confiscation, the ownership of the company is transposed to Türkiye's government (Ministry of Treasury). MoT assesses the asset and chooses between continuing managing the company and liquidating it. If the liquidation is decided, the company is sold, and the gain goes into the general administration budget.
b) Between 2021-2025, a total of 815 companies and businesses were subject to SDIF's receiver administration, including 480 joint stock companies, 273 limited companies, and 62 other types of companies and businesses.
c) Liquidation of the asset or legal persons: this measure is applied when there is a likelihood that a seized item will be damaged or suffer a substantial loss of value, the item in question may be liquidated before final judgment.
d) PPOs custody applies for the movable assets subject to seizure. While cash is immediately deposited in an interest-generating bank account, gold, precious stones and equipment that must be physically preserved are taken in custody warehouses until the criminal investigation is finished and the confiscation or devolution is ordered.
e) For VAs, since June 2025, public prosecutors are instructed to sell all VAs seized at market price, convert them into TRY and immediately deposit the cash into an interest-generating bank account without waiting for the completion of the investigation and prosecution. Before, public prosecutors

transferred the VAs into public wallets under the PPOs. The new management system was enacted considering the high-risk of VAs, their volatile nature and the of the risk in VA based in the strategy document to enhance the fight against ML/TF.

f) Goods that are seized or confiscated and/or abandoned at the Customs Enforcement facilities are transferred to Treasury and subjected to liquidation. For these cases, the liquidation procedures are carried out by the General Directorate of Liquidation Services (TASİŞ), a revolving fund enterprise operating under the Ministry of Trade. TASİŞ is responsible for the sale (via e-auction, public auction, or retail), allocation to public institutions, destruction, or recycling of such goods. Sales are conducted both electronically through online and physically at designated retail stores operated by TASİŞ. Goods deemed unsuitable or hazardous to health are destroyed in accordance with environmental regulations.

8.5. Confiscating and enforcing confiscation orders

8.5.1. Criminal property and property of corresponding value located domestically

508. Türkiye is able to confiscate and enforce orders on criminal property and property of corresponding value located domestically. However, the size of assets recovered appears to be modest given Türkiye's risk and context.

509. For an asset to be subject to confiscation, it must either constitute the object of the offence, be derived from the offence, be used in its commission, or be intended for its commission. Additionally, any property whose production, possession, use, transportation, purchase, or sale constitutes an offence shall be confiscated directly, without the need to meet the above conditions. Between 2021 and 2025, Türkiye confiscated above EUR 93 M (see table 8.2) which demonstrates Türkiye's ability to convert seizures into final confiscations to some extent. In addition, a total of 560 assets (see table 8.3), including vehicles (36%), bank and other type of FIs accounts (12%) and immovable properties (12%). The low number of banks and other FIs accounts remains a concern given Türkiye's' risk profile (see IO.1 and IO.3). In addition, it was not possible to distinguish if the confiscated assets were located domestically or abroad.

510. In addition to confiscation measures conducted under a criminal process, complementary administrative mechanisms are also employed to deprive criminals of illicit assets. These include the seizure and detention of smuggled goods under the Customs Law and Anti-Smuggling Law, as well as tax audits and fines arising from tax evasion inspections. These measures are implemented concurrently. Since the benefits derived from tax crimes are followed up by the Tax Board, a confiscation decision cannot be made regarding the income derived from these crimes. However, recovery of the illicit benefit is largely pursued through the tax administration via tax assessments and penalties, rather than through criminal confiscation. Tax fines represent nearly 75% of the total tax revenue collected by the country.

511. Non-conviction-based confiscations (NCBC) are applicable when the offence perpetrator is a fugitive, unknown or abroad, or in case of death if the legal requirements are met. In these cases, NCBC is applicable to items whose production, possession, use, transport, purchase or sale constitute an offence. Türkiye has applied NCBC in one case. Türkiye can also apply an 'additional indictment' (post-conviction confiscation) procedure to extend confiscation to assets linked to prior convictions. This process does not equal a general confiscation an/or other assets that cannot be proven to be linked to the prior conviction. However, due to the limited information on the implementation of such measures, their effectiveness cannot be assessed.

8.5.2. Criminal property and property of corresponding value located abroad

512. Türkiye enforces confiscation orders from abroad (see IO.2) and has demonstrated through case studies to be able to repatriate assets from abroad to a limited extent.

513. When an asset located outside Türkiye is identified, public prosecutors develop a strategy to engage with their counterparts in the foreign jurisdiction and establish both informal and formal co-operation mechanisms to request the freezing, seizure, or confiscation of the asset (see IO.2). Informal co-operation mechanisms are generally initiated to identify the asset and develop a financial assessment of the suspect (i.e., bank accounts, travel history, nationality, whether dual citizenships or not) prior to issuing the MLA order. The aim is not only to trace the identified asset but also to expand the search to all other possible assets the suspect owns or holds outside Türkiye. When assets are identified, public prosecutors initiate the formal MLA process requesting the freezing, seizing or confiscation as needed.

514. Between 2021-2025, Türkiye requested the seizure of assets located abroad on a few times (eight) and initiated the formal MLA confiscation process in limited times (two). These two confiscation cases resulted in historical artifacts smuggled from Türkiye being successfully confiscated and repatriated. The low number of requests to execute freezing, seizure, and confiscation of assets abroad highlights the limited application of cross-border asset tracing and enforcement of seizure and confiscation measures.

8.6. Returning confiscated property to victims

515. In principle confiscation revenues cannot be allocated directly for the compensation of the victims and these revenues need to integrate into the government general budget. However, there are four exceptions to this rule where victims can be compensated for their losses: remorse provisions, alternative sanctions applied to the criminal, settlements and civil lawsuits.

516. Türkiye has returned a large number of assets and funds subject to seizure and/or confiscation to identified victims (EUR 151 M). Most of the returned assets relate to fraud and forgery (92%), followed by drug trafficking (3.6%) and theft cases. The value of assets returned to victims (EUR 151 M) is nearly twice the total value of assets confiscated (EUR 93 M). Türkiye authorities explains this disparity stating that confiscation of assets is not possible where seized assets belong to a victim whose identity is known, as such assets must be returned to the victim. Final confiscation by the government is only permitted where restitution is not possible and for specific offences (see table below). Similarly, seized assets belonging to third parties are returned when they are no longer required for the purposes of the investigation or prosecution, or when they are not subject to confiscation. In this context. However, this deficiency continues to raise concerns as the disparity highlights the limited application of confiscation measures.

Table 8.4. Overall assets returned to victims (2021-2025)*

Year	Fraud & Forgery (EUR)***	Drug Trafficking (EUR)	Theft (EUR)	Human Trafficking (EUR)	Illegal betting (EUR)	Arms trade (EUR)	Damage to property (EUR)
2021	€ 188,452.76	€ 32,607.33	€ 111,369.29	€ 11,005.14	€ 18,863.59	€ 32.98	€ 1.46
2022	€ 569,125.34	€ 23,936.18	€ 69,503.81	€ 12,295.58	€ 1,271.56	€ 3,485.38	€ 91.54
2023	€ 118,220,723.32	€ 860,962.44	€ 1,849,124.40	€ 152,507.70	€ 533,757.15	€ 83,852.67	€ 91,854.68
2024	€ 7,698,562.40	€ 1,905,334.34	€ 1,064,846.13	€ 257,773.40	€ 114,561.58	€ 44,814.84	€ 36,764.88
2025**	€ 12,350,124.09	€ 2,578,686.31	€ 1,601,836.36	€ 523,317.59	€ 22,364.68	€ 222,022.14	€ 23,470.01
Total	**€ 139,026,987.91**	**€ 5,401,526.60**	**€ 4,696,679.99**	**€ 956,899.41**	**€ 690,818.56**	**€ 354,208.01**	**€ 152,182.57**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025); (***) Conversion rates were calculated on annual average bases as follows: year 2020 (1 TRY=0.12 EUR); year 2021 (1 TRY= 0.097 EUR); year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); year 2024 (1 TRY= 0.028); and year 2025 (1 TRY= 0.022 EUR).

8.7. Identifying and confiscating falsely or undeclared currency/BNIs or those related to ML/TF or predicate offences

8.7.1. Identifying and seizing non-declared or falsely declared cross border movements of currency and BNI

517. Türkiye has a hybrid system (cash declaration and disclosure systems) in terms of seizing non-declared or falsely declared cross-border currency movements. Despite Türkiye's efforts in resourcing Customs Enforcement checkpoints with the highest technology, in line with its ICRG Action Plan, the number of non-declared or falsely declared cross-border currency and BNI movements detection and seizure remains limited. This is not aligned with the country's risk profile as cash-smuggling is rated as a medium risk in the 2025 NRA.

518. Customs Enforcement is the competent authority accountable for receiving cash declarations and disclosures, detecting illegal cross-border movements of currencies and BNIs and seizing them at border check points. Türkiye has demonstrated a stable increase in cash declarations and disclosures since 2021. See below:

Table 8.5. Cash declaration and disclosure reports (2020-2025)

	Cash declarations				Cash disclosures			
	Incoming		Outgoing		Incoming		Outgoing	
Year	No. Transactions	Amount (EUR)**	No. Transactions	Amount (EUR)	No. Transactions	Amount (EUR)	No. Transactions	Amount (EUR)
2020	14765	€7,364,160.,755	1030	€1,347,734,215	117	€45,085,575	1378	€ 5,049,663
2021	25601	€21,480,648,592	3658	€3,219,262,980	10340	$213,296,666	17067	€12,482,095
2022	31344	€23,976,412,012	5798	€6,922,315,173	14874	$56,205,333	29146	€19,458,874
2023	32339	€19,793,870,221	6174	€8,410,409,850	5928	$35,787,546	16086	€11,688,858
2024	19175	€8,402,391,339	4211	€2,568,120,646	12156	$47,884,222	15366	€9,701,931
2025*	9475	€6,859,573,745	3200	€2,967,308,686	11060	$37,298,362	19528	€19,021,589
Total	**132699**	**€87,887,056,601**	**24071**	**€25,435,151,551**	**54475**	**$435,557,704**	**98751**	**€77,403,010**

Note: (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025); (**) Conversion rates were calculated on annual average bases as follows: year 2020 (1 TRY=0.12 EUR); year 2021 (1 TRY= 0.097 EUR); year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); year 2024 (1 TRY= 0.028); and year 2025 (1 TRY= 0.022 EUR).

519. To improve the identification of non-declared or falsely declared cross-border movements of currency and BNI, CE has invested significantly in technical equipment including advanced technology, such as drones and tomographic luggage X-ray devices. In addition, 17 money counting machines with features such as distinguishing counterfeit money, recording serial numbers of money and counting more than one currency at the same time, have been provided to provincial administrations to carry out cash control operations in a reliable and fast manner. Competent authorities highlight this investment as significant improvements in the detection of cash smuggling. In 2016, the CE has established a certified World Customs Organisation K9 training facility to train cash, narcotics, tea/tobacco and explosive detector dogs. Between 2021-2025, CE trained a total of 11 268 officers in charge or passengers operations cash control trainings. Competent authorities report that these investments have led to an increase in cross-cash interceptions at customs checkpoints.

520. CE carry out controls upon entry to and exit from the country. Customs officers can physically verify the declared amount of currency were deemed necessary (i.e., when observing red flags, inconsistencies, or behaviour-based alerts). In such cases, the cash may be inspected, counted, and compared against the

declared figure. If a passenger has failed to declare or made a false declaration or disclosure, the CE officer completes a new declaration form reflecting the accurate amount, the cash is seized, and the case is reported to the public prosecutor. A copy of the case file, including the declaration form and seizure records, is transmitted to MASAK in accordance with the reporting obligations. This reflects the existence of financial monitoring at border points aimed at identifying potential ML risks associated with cross-border movements. However, the number of opened cases remains limited (506) given Türkiye's medium level of cash smuggling.

521. In addition to the declaration system, Türkiye operates a disclosure system that allows customs officers to request information from passengers regarding the cash or payment instruments they carry. Under this framework, passengers may be invited to make a disclosure by customs officers based on risk profiling, behavioural red flags, or random selection, regardless of whether the amount carried exceeds a legal threshold. Officers may request details about the amount, origin, and intended use of the funds upon entry to or exit from the country, and the process is not limited to specific types of currency or financial instruments. If a passenger refuses to respond, or provides a false or misleading explanation upon request, a Cash Disclosure Report is drawn up and signed by at least two customs officers and the passenger. This report is forwarded to MASAK, and the case is also submitted to the Public Prosecutor. If a violation is confirmed, the undeclared or miss declared funds are seized.

522. In situations where the cash or other items being transported include foreign exchange, securities, precious metals, or other high-value instruments and the act involves unauthorized import or exports procedures, administrative fines can also be imposed up to the full value of the goods, or 50% in case of attempt unless the conduct constitutes a smuggling offence.

523. Between 2020 and 2025, CE have identified and seized non-declared and falsely declared currency for a total of EUR 85.2 M in land and airport customs controls points. The currencies more frequently seized are US dollars, Turkish lira and Euros. Within the scope of cash controls, suspicious indicators such as the unusual behaviour of individuals carrying cash, the presence of large-denomination banknotes (e.g., EUR 200 and EUR 500), concealment of money on persons or in vehicles, and disproportionate transaction volumes conducted by companies relative to their declared business activities are monitored closely. In addition, data derived from risk analyses conducted on legal entities and transaction patterns are evaluated. When such elements raise suspicion, reports are submitted to the judicial authorities, and the MASAK is granted access to the related data to conduct further financial analysis on potentially high-risk individuals, transactions, or corporate entities. The number of such reports submitted by year is presented in the table below.

Table 8.6. Cash seizures at CE checkpoints leading to notifications to MASAK (2020-2025)*

Year	Number of transactions	Cash Seized (EUR)**	Notifications to MASAK
2020	55	€ 15,025,403	0
2021	52	€7,421,798	1
2022	58	€10,592,182	1
2023	72	€13,763,745	19
2024	139	€21,680,024	76
2025	130	€16,721,928	366
Total	**506**	**€85,205,081**	**463**

Note: (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025); (**) Conversion rates were calculated on annual average bases as follows: year 2020 (1 TRY=0.12 EUR); year 2021 (1 TRY= 0.097 EUR); year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); year 2024 (1 TRY= 0.028); and year 2025 (1 TRY= 0.022 EUR).

524. The significant higher volume of incoming cash declarations (EUR 87.9 billion) compared to outgoing ones (EUR 25.4 billion), and the incoming cash disclosure (EUR 435 M) and outgoing (EUR 77 M), coupled with minimal seizures and the high risk of smuggling, indicates limited effectiveness of the existing control measures. In addition, the predominance of inbound declarations and the dissemination of only 506 reports to MASAK, while seizing 463 times in customs gates, suggests potential gaps in enforcement and risks management at entry points.

8.7.2. Confiscation of currency or BNI related to ML/TF or predicate offences

525. Türkiye authorities have shown they can confiscate currency or BNIs where they considered there is a link to ML/TF or associated predicate offences through six case studies. While the competent authorities have seized foreign currency, cash, and goods (notably gold and technology) to some extent and have, where relevant, initiated criminal investigations, they are not able to demonstrate that these seizures are linked to money laundering, terrorist financing, or specific predicate offences. This points to limitations in Türkiye's ability to effectively identify and substantiate ML, TF, or related predicate offence typologies when pursuing confiscation orders when assets are being seized as a result of the application of CE enforcement measures.

8.7.3. Sanctions

526. For cash disclosure an administrative fine equal to 10% of the difference between the declared and actual amounts is imposed on the traveller. However, if the discrepancy is below EUR 1 000 (50 000TRY), no penalty is applied. Sanctions effectiveness was not measured due to the lack of information.

Table 8.7. Cash seized based on CE sanctions imposed (2020-2025)

Year	Value Seized (TRY)	Value Seize (EUR)**
2020	₺ 10,737,242	€ 1,288,469
2021	₺ 19,723,944	€ 1,913,223
2022	₺ 35,830,821	€ 2,042,357
2023	₺ 147,542,972.00	€ 6,049,262
2024	₺ 72,466,244	€ 2,029,055
2025*	₺ 70,170,782	€ 1,543,757
Total	**₺ 356,472,005**	**€ 14,866,122**

Note: (*) 2025 figures reflect information available up to the end of the on-site visit (November 2025); (**) Conversion rates were calculated on annual average bases as follows: year 2020 (1 TRY=0.12 EUR); year 2021 (1 TRY= 0.097 EUR); year 2022 (1 TRY= 0.057 EUR); year 2023 (1 TRY=0.041 EUR); year 2024 (1 TRY= 0.028); and year 2025 (1 TRY= 0.022 EUR).

9 Terrorist financing investigations and prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.9 The Recommendations relevant for the assessment of effectiveness under this chapter are R. 5, 30, 31 and 39 and elements of R. 1, 2, 15, 32, 37 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Türkiye has strong and institutionalised capabilities to identify and investigate TF in relation to terrorist organisations, associated individuals, groups, undertakings and entities designated by the United Nations Security Council (UNSC)[34] and those designated under its national regime. All CT/CFT competent authorities have a sufficient degree of specialisation to identify and investigate TF and are well equipped to assess and identify TF activity in the context of broader terrorism investigations. PFIs are mandatory in all terrorism cases since 2020 and are systematically applied. Operational detection is further supported by extensive information-sharing arrangements and integrated databases, which facilitate rapid access to financial intelligence, travel data, and criminal justice records, strengthening investigative workflows across competent authorities.

b) Türkiye's operational focus covers a broad range of TF activities and typologies, including traditional and evolving methods such as VAs, informal value transfer systems (hawala), social media, abuse of NPOs and commercial entities linked to FETÖ-related cases. This demonstrates an ability to detect and investigate different forms of TF activity. However, the demonstrated casework is uneven across Türkiye's broader TF risk profile. A significant share of investigations concerns lower-value individual donations, ATM micro-transfers or minor facilitation, while further demonstration is needed of cases involving layered commercial, trade-related or legal person structures beyond the FETÖ-related casework.

c) Türkiye has investigated, prosecuted and convicted a substantial number of TF cases,

[34] Pursuant resolutions 1267(1999), 1989 (2011) and 2253(2015) concerning the Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities.

particularly in relation to UNSCR-listed and domestically designated terrorist organisations, with over 11 000 investigations, 2 500 prosecutions and more than 400 convictions between 2021 and 2025[35]. However, Türkiye has not demonstrated TF investigations, prosecutions or convictions involving terrorist organisations and networks that are not subject to designation under UNSCRs[36] or Türkiye's domestic regime but are identified through international sources and co-operation channels as relevant to its TF risk exposure. The only demonstrated activity in this area relates to two responses to foreign requests for information. This represents a significant effectiveness gap and materially limits the extent to which it can be concluded that Türkiye is effectively identifying and pursuing TF activity across the full scope of its relevant TF risk environment, including those arising from its role as a regional financial, trade and logistics hub.

d) Türkiye has a robust sanctioning framework for natural persons convicted of TF offences which is considered effective, proportionate and dissuasive. While legal persons are not subject to criminal liability, security measures and administrative sanctions are available and have been applied. However, their use remains limited and does not reflect the materiality of legal persons and complex commercial structures in Türkiye's TF risk environment.

e) Türkiye deploys a wide and active set of alternative measures where TF conviction is not feasible, including alternative criminal charges, deportation, administrative asset freezing and transaction postponements, and has demonstrated their use in practice. However, the extent to which these measures contribute specifically to the disruption of TF activity, including their impact on the underlying financial aspects of TF networks, is not fully demonstrated.

f) Türkiye has a well-developed domestic CT/CFT strategy, with structured inter-agency mechanisms and policy documents which are informed by and periodically reviewed on the basis of operational findings. However, evidence of how TF intelligence is systematically leveraged for operational CT purposes, including targeting, designations and disruptions, is more limited.

[35] 2025 figures reflect information available up to the end of the on-site visit (November 2025).

[36] Notably Hamas.

Key Recommended Actions (KRAs)

Türkiye should

r) Improve the identification, investigation and, where appropriate, the pursuit of prosecutions and convictions linked to the full range of TF threats aligned with their up-to-date risk profile. This should include operational guidance, case-handling standards and specialised training focused on risk-based identification of illicit activity beyond formally designated terrorist entities.

s) Further develop the identification, investigation and prosecution of complex TF cases, including trade-based TF, large-scale procurement networks and layered cross-border financial structures.

t) Strengthen the investigation and sanctioning of TF involving legal persons and commercial structures, including by increasing the use of security measures and administrative sanctions, to ensure broader and more consistent application beyond the FETÖ-related cases demonstrated.

Other Recommended Actions

a) None.

Overall Conclusions on IO.9

Türkiye has significantly increased TF investigations, prosecutions and convictions since the previous MER in relation to UNSCR-listed and domestically designated terrorist organisations. Türkiye has strong national co-ordination settings, legal framework, national policies, and specialised personnel to successfully identify, investigate, prosecute and convict a broad range of TF activities. Public prosecutors and courts have demonstrated the implementation of effective, proportionate and dissuasive sanctions for natural persons, while sanctions imposed on legal persons remain more limited.

Competent authorities demonstrate a solid understanding of TF threats and vulnerabilities related to UNSC-listed and domestically designated terrorism threats and are consistently trained in the terrorist organisations financing methods. Türkiye has specialised courts, public prosecutors, LEAs, and dedicated FIU units to support TF investigations and prosecutions. The systematic use of parallel financial investigations (PFIs) in all terrorism cases since 2020 is a major operational strength and has contributed to a substantial increase in TF prosecutions and convictions.

Türkiye's operational focus covers a broad range of TF activities, including both traditional and evolving TF methods and aligns with the TF threats identified in its NRA (FETÖ, PKK/KCK-PYD/YPG, ISIL, AQ). Türkiye also demonstrates engagement in international TF cases, including both domestically initiated and externally triggered investigations. However, the demonstrated casework is not equally developed across all relevant risk areas. A significant share of investigations and outcomes concerns lower-value individual donations, ATM micro-transfers and minor facilitation. Further demonstration is needed of effective outcomes involving trade-based TF, the abuse of MVTS and exchange houses, large-scale procurement networks, complex use of legal persons and complex commercial structures beyond FETÖ-

related cases.

A significant effectiveness gap remains in relation to terrorist organisations and networks that are not designated under UNSCRs or Türkiye's domestic regime but are identified through international sources and co-operation channels as relevant to Türkiye's TF risk exposure. No investigations, prosecutions or convictions were demonstrated in relation to such entities. The only demonstrated activity in this area relates to responses to foreign requests for information. This materially limits effectiveness, as it constrains Türkiye's demonstrated ability to identify and pursue TF activity across the full spectrum of its relevant TF risk environment.

Türkiye uses a range of alternative measures where a TF conviction is not practicable, including alternative criminal offences, migration-related measures, administrative freezing and transaction postponements. These tools are available and used in practice, but their structured application as substitutes for TF convictions and their specific contribution to disrupting TF activity are not fully demonstrated.

Türkiye is rated as having a Moderate level of effectiveness for IO.9.

Immediate Outcome 9

527. Türkiye is directly targeted by and exposed to the threat of a number of domestically designated and UNSCR-listed terrorist organisations and individuals which use a wide range of mechanisms to raise, move and spend funds. Türkiye is also exposed to TF risks arising from terrorist organisations and networks not subject to designation under UNSCRs or Türkiye's domestic regime but identified through international sources and co-operation channels as relevant to its TF risk exposure.

528. Although Türkiye's materiality and institutional factors have changed since its 2019 MER, Türkiye's geographical location remains a major contextual factor influencing the risk of TF. Türkiye's proximity to armed conflicts, its extensive land borders with neighbouring countries also exposed to high terrorist and terrorist financing threats and its role as a regional financial, trade and logistics hub expose it to risks of being used as a transit, procurement or financial channel for terrorist organisations and networks. Terrorist organisations use sophisticated financing schemes which include physical transportation of cash, VAs, Hawala, trade-related activities and the abuse of different AML/CFT regulated sectors to channel funds or other assets into or through Türkiye's financial system. Through the creation of multilayered legal businesses (including enterprises and real estate investment schemes), these organisations store and/or multiply their assets to subsequently outflow them among others in the form of gold, cash, goods, or VAs to other jurisdictions to support their operational needs.

9.1. TF activity identified and investigated

9.1.1. Identification and investigation of TF activity

529. Türkiye has well-developed and institutionalised capabilities to identify and investigate TF for risks related to TOs, associated individuals, groups, undertakings and entities designated by the UNSC[37] and those designated under its national sanctions' regime. Türkiye's operational focus covers a wide range of TF activities, including a combination of traditional and evolving TF methods, and aligns with the TF threats

[37] Pursuant resolutions 1267(1999), 1989 (2011) and 2253(2015) concerning the Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities.

identified in its NRA (FETÖ, PKK/KCK-PYD/YPG, ISIL, AQ). However, Türkiye has not demonstrated investigations involving TOs and networks not subject to designation under UNSCRs or Türkiye's domestic regime but identified through international sources and co-operation channels as relevant to Türkiye's TF risk exposure. This limits the demonstrated ability to identify TF activity across the full range of Türkiye's relevant TF risk environment.

530. Türkiye identifies TF activity through different operational tools, including (i) broader terrorism investigations; (ii) domestic operational detection channels; (iii) foreign intelligence sharing or co-operation requests; and (iv) detection of positive matches when screening against sanctions lists. While the overall detection ecosystem is robust, foreign intelligence has triggered relatively few domestic TF investigations, and the demonstrated use of foreign-generated information is strongest where the relevant terrorist organisation or network corresponds to Türkiye's designated threat profile (see also table 9.2 below).

531. All CT/CFT competent authorities have a sufficient degree of specialisation to identify and investigate TF and are well equipped to assess and identify TF activity in the context of a broader terrorism investigation. PFIs are the most common method of detecting TF activity in the country. When a new TF trend or activity is detected, the Threats and Vulnerability WG discusses the case and the indicators for detection to design a holistic strategy to disrupt the activity including all relevant CFT authorities.

532. Türkiye demonstrates a strong use of a wide range of sources of information to initiate TF investigations as TF activity detection also arises from MASAK analytical outputs, LEA and intelligence agency information (mainly from TNP and GGC), social media monitoring, and border/security operations. The specific channels include: reports from local and foreign counterparts' intelligence units, financial networks analysis of individuals linked to terrorist organisations, information from customs and migration offices, and a broad access to different sources of information, including open-source intelligence information (OSINT) and social media monitoring, examination of the financial movements of associations, foundations, companies, or aid organisations affiliated with terrorist organisations, examination of evidence seized during judicial or rural terrain operation against terrorist organisations (bank statements, VAs data, etc.), reviews of existing databases and anomaly studies created in AI-supported databases, examination of all types of smuggling activities and their connection to terrorist organisations; and typologies obtained from international reports. TF activity is also detected when conducting the verification of the positive matches arising from screening against sanctions lists. Once the positive match is reported, a financial investigation is conducted against the listed person or entities and their relatives.

533. Türkiye identifies a range of complex TF typologies, including the use of VAs, hawala networks, social media, abuse of NPOs, and commercial entities linked to FETÖ, demonstrating an ability to detect sophisticated TF schemes. However, a significant share of investigations concerns lower-value individual donations, ATM micro-transfers or minor facilitation. This is acknowledged as a common feature of TF networks, which often include many low-level contributors and fewer central collectors or co-ordinators. Nevertheless, given Türkiye's broader risk profile as a regional financial, trade and logistics hub, further demonstration is needed of investigations involving TBTF, large-scale procurement networks and complex use of legal persons beyond the FETÖ-related commercial structures demonstrated.

534. Türkiye has demonstrated strong use of interagency information sharing mechanisms and broad access to TF-related information, enabling competent authorities to take timely action to disrupt TF activity. Türkiye has established formal mechanisms for information sharing through interagency MoUs, including between prosecutors, LEAs, MASAK, and other competent authorities. Ad hoc interagency teams can be constituted for specific investigations or to address a developing trend. Through the dedicated UYAP system, public prosecutors can access in a single platform a wide range of information, including bank account and transaction data, travel information, and criminal-justice records, enabling rapid cross-checking of financial footprints, travel, communications, and criminal records. This is a major operational strength.

535. Although most TF investigations originate from domestic intelligence sources in the context of a broader terrorism-related investigation concerning UNSC-listed or domestically designated organisations, Türkiye has a well-established mechanism to identify related foreign-linked TF activities, relying mainly on informal bilateral and international co-operation processes. For this purpose, competent authorities use LEA co-operation networks (bilateral agreements and INTERPOL channels), legal liaison officers posted in Türkiye's embassies, and FIU co-operation mechanisms, including the EGMONT Group (see IO.2).

Box 9.1. TF investigation triggered by an international request led to an international ISIL activity disruption case.

TNP TEM-CFT Division: Case "Open Radar"

In 2025, TNP-TEM received a co-operation request from its liaison officer posted in a European country in relation to seven Turkish nationals being investigated for collecting funds for ISIL members in Syria. The suspects allegedly organized crowdfunding campaigns and collected money via instant messaging application channels, which was then transferred to Syria to support ISIL prisoners.

TNP in co-ordination with the FIU, TNP cyber units and intelligence agencies, expanded the analysis of seven Turkish nationals and conducted a financial investigation. As a result of these co-ordinated efforts, 82 suspects were detected, of whom 43 were Turkish nationals and 39 foreigners. 22 of the total suspects had criminal records related to terrorism offences, 10 were subject to investigation in a European country, 5 had assets frozen in Türkiye and 4 were on a wanted list for terrorism offences.

The results were communicated to the Public Prosecutor's Office who initiated the TF investigation. The parallel financial investigation concluded that suspicious transactions were made by four of the suspects through electronic payment companies and by using VASPs in different currencies (EUR, USD, TRY) totalling EUR 312 000 over a period of six years. All transactions had a common coded pattern and had no business justification or linkages. Transactions also included high value cash withdrawals. In a co-ordinated operation led by the public prosecutor and enforced by TNP TEM, 15 suspects were arrested, digital material, documents and EUR 12 320 were seized.

All operational results were communicated to the requesting country and prosecution is ongoing.

536. Most financial information and intelligence requests are related to tracing, profiling, transactions records and asset freezing purposes. For foreign linked TF activity, many requests relate to information exchange on foreign individuals' entry and exit information, addresses, citizenships, and financial profiles. Türkiye has presented some cases, in which it has successfully responded to foreign counterparts' investigations and asset freezing requests, including in a small number of instances involving terrorist entities that are neither UNSC nor domestically designated by Türkiye. Türkiye provided only two such cases for assessment (see Box 9.2 below), which limits the ability to evaluate the scope and consistency of this practice; no aggregate figures were provided.

Box 9.2. International responses to foreign intelligence requests related to entities designated unilaterally by other jurisdictions (neither UNSC nor domestically designated by Türkiye).

Case 1:

In 2023, Country X requested information from Türkiye through the Egmont Group in relation to a real estate investment partnership established in 2013, and some of its partners, which were suspected of exploiting the real estate sector and financial sector in Türkiye for the purpose of raising and transferring these funds to an entity that was not UNSC-listed but had been unilaterally designated by Country X domestically.

Türkiye's FIU initiated a financial analysis in response to the request on the company and its partners, including a review of the statement made to the Public Disclosure Platform (KAP), open-source intelligence and financial data from the FIU's databases. The analysis revealed that 25 % of the company's shares are publicly traded on the Istanbul Stock Exchange and that the company is subject to independent audit in accordance with the Capital Markets Law and the TCC. Furthermore, it was understood that following a unilateral designation by Country X, partner's duties at the company have been terminated and their shares have been transferred to the other partners.

The investigation concluded the company's current partners did not hold partnerships in other companies, had no registered criminal records. No significant or unexplained high-value cash inflows or outflows were identified in their account, and no notifications had been received from financial institutions indicating individuals had been listed by any jurisdiction other than the requesting country. Regarding the company's accounts, no transfers of funds of significant size or from unknown sources, whether domestic or foreign, were identified, and it was determined that the transfers recorded in the accounts were consistent with the company's declared field of activity.

A summary of the analysis results was shared with the requesting country in accordance with Egmont Group principles.

Case 2:

In 2024 an EU country filed an urgent information request through the Egmont Group on a target (Mr A) indicating that he was suspected of financing illegal organisations abroad. The requesting country was particularly seeking to determine whether Mr A had any financial transactions with Mr B, who according to open-source information, was one of the "central figures" of a non-UNSC-listed entity in the country. The media reports indicated that Mr B was allegedly arrested on terrorism and terrorism financing charges.

MASAK and the requesting country's FIU held consultations to discuss the case details following which MASAK conducted a financial analysis of the individuals concerned and replied to the request with all available information. According to the analysis Mr B had been subject to judicial proceedings in a third country and was acquitted of all alleged terrorism and terrorism financing charges. No further information was received from the requesting country.

537. In addition, Türkiye has utilised foreign intelligence in investigations to identify TF activities related to its main TF threats resulting in concrete enforcement actions. Türkiye has a system in place to integrate all foreign financial information (i.e., migration information, bank accounts, criminal records) into the UYAP system with the objective of integrating it into the national records. Both domestic and foreign intelligence sources are evaluated and incorporated as evidence when appropriate. However, the integration of foreign-

generated intelligence is more limited. The table below shows the number of times in which foreign intelligence was integrated into TF files processed by the FIU and disseminated to LEAs.

Table 9.1. Cases of foreign intelligence provided through EGMONT Group integrated into TF files analysed by MASAK and disseminated to LEAs (2021-2025)*

Year	Number of files	Number of persons subject to analysis
2021	73	189
2022	84	120
2023	68	138
2024	90	198
2025**	61	144
Total	**376**	**789**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

538. Public prosecutors lead TF investigations and are responsible for setting the strategic direction of the case and decide which LEAs will assist to produce evidence to support the investigations. Following the priorities established by the National CFT Strategy, the Council of Judges and Public Prosecutors assigned more than 100 specialised public prosecutors to TF investigations. These prosecutors are distributed across all 81 provinces including at least 1 in each province and more than one in metropolitan cities.

539. Public prosecutors handling TF investigations and LEAs routinely identify whether a suspect: (a) collects funds (through donations, coercive fundraising, diaspora channels, VAs, and crowdfunding campaigns); (b) moves funds (through hawala chains, payment institutions, VASPs, front companies, and couriers); or (c) uses funds (for procurement, logistics, payment to fighters, family support, and operational expenses).

540. PFIs are systematically opened for all terrorism files. Following a MoJ Circular, this policy has been adopted in 2020 and led to PFIs being conducted in around 60% of cases in 2020 up to 100% in 2025. Public prosecutors can initiate an investigation under the simple suspicion of TF activity. PFIs are conducted to determine whether each suspected TO member or individual is also able to provide, collect or hold funds for the organisation. PFIs, involve a thorough review of suspects' and their family members' assets (including analysis of movable and immovable property, bank accounts, and VAs) to assess consistency with declared income and business activities. The goal is to identify disproportionate wealth, trace asset sources, and uncover links between financial accounts and terrorist organisations. PFIs also focus on the examination of physical evidence such as diaries, receipts, and bank cards seized during searches, as well as social media activity and personal networks to detect hidden financial channels or affiliations. In addition, all investigations conducted for searching, seizing and confiscating proceeds of crime shall also include research whether the investigated persons are affiliated with any terrorist organisation, and whether they used proceeds of crime for financing any terrorist organisation or terrorist act.

541. Competent authorities co-operate to a large extent for detecting and identifying TF activity. Public prosecutors generally rely on TNP and GGC CT/CFT specialised units to support most of the investigations as they have a vital role in the prevention of both terrorism and TF activity. For complex TF cases, public prosecutors also request the production of financial analysis and intelligence from the FIU. Throughout the course of the investigation, all competent authorities co-ordinate their enforcement actions creating *ad hoc* joint investigations teams led by the public prosecutors. Public prosecutors also request support from the CGC in case of TF activity detected in maritime areas and CE Agencies when the TF activity is being detected at points under customs supervision, including borders, ports and airports.

542. Competent authorities are well-equipped to detect and investigate TF and work together in a highly co-ordinated and complementary manner. The main CFT structures in place for supporting TF and parallel financial investigations are as follows:

b) The TNP and its specialised TEM unit have sufficient staff to conduct TF-focused investigation in addition to their general duties.[38] The TNP TEM unit has sub-units specialised in each terrorist organisation identified as a threat in the NRA, i.e. UNSCR-listed and domestically designated organisations. In addition to TEM, the anti-smuggling and organised crime unit (KOM) manage TF cases related to FETÖ organisation with the help of 52 officers. Between 2021-2025, TNP has sent 9 written orders covering 81 cities/ TNP TF Branches in Türkiye on the importance of revealing the financial structures of terrorist organisations, prioritizing the financing of terrorism, the use of social media and VAs by terrorist organisations, terrorist financing typology guides, raising funds for terrorist organisations with proceeds of crime and increasing the effectiveness of TF investigations.

u) GGC is competent in supporting CT/CFT investigations when occurring in rural areas. The GGC Anti-Terrorism Financing Branch Directorate (GGC TEM) employs around 1 500 personnel across headquarters and provincial CT units. Of these, 136 officers (8 at headquarters and 128 in the provinces) are fully dedicated to combating TF, while the remaining staff carry out broader CT and CFT duties. Most of the latter have received training on TF, enabling them to participate in CFT-related operations as part of their general CT responsibilities. The GGC TEM has sub-units specialised in each relevant terrorist organisation following the NRA findings (i.e., those organisations listed under the UNSCRs or domestically designated by Türkiye). The GGC TEM can access cross-border movement information allowing LEAs to add information on the dates of entry/exit of the person/suspect at the country's land borders, the amount and type of cash they carry, flight entry/exit information, identification of persons traveling with them, membership information of foundations/associations, providing access to social security institution records and job data, which contributes to creating a full profile of the suspect.

v) CGC has a responsibility for combating all sea border related crimes with over 8 002 officers. After the 2019 MER, the Coast Guard established the first TF Section Chief transformed into a TF Branch Directorate in 2024 to increase the focus on TF-activity detection, allocating 31 officers in the headquarters office and 169 in the provinces.

w) CE have responsibilities with respect to smuggling activity detected at points under customs supervision, including borders, ports, and airports. Customs Enforcement has no dedicated TF unit; in cases of TF-related suspicion, officers report to the Public Prosecutor and MASAK. Given the significant TF risks associated with trade-based activity and cash smuggling at borders, ports, and airports the absence of a specialised TF capacity within Customs Enforcement is a relevant limitation.

543. MASAK plays an important role in contributing to TF investigations when proactively disseminating financial intelligence to the public prosecutor's offices and when contributing with case-specific financial analysis when requested by a public prosecutor in the context of an investigation. MASAK has 44 officials dedicated to the analysis of TF activity distributed in two different units: (i) Terrorism Financing Analysis with 22 analysts and (ii) Terrorism Financing Analysis Department also with 22 analysts. While both departments conduct analysis on FETÖ, the first department conducts analysis on UN-listed terrorist organisations such as ISIL/Al-Qaida and organisations which abuse religion, and the second department conducts analysis on PKK/KCK-PYD/YPG. TF examinations can be triggered by various sources of information (see earlier in this Chapter and IO.6 analysis).

[38] The employee figures were submitted to the assessment team, but the state's request to refrain from publishing them due to their sensitive nature was considered

544. All LEAs are extensively trained to detect and disrupt terrorist financing activity. Türkiye provided through MOJ, MASAK and the relevant LEAs almost 217 CFT-related trainings, courses, workshops and drill scenarios when applicable. The table below shows the number of CFT trainings delivered and participants:

Table 9.2. CFT Trainings delivered to operational experts (2020-2025)*

Year	Item	MOJ	MASAK	TNP	GGC	Customs Enforcement	Coast Guard
2021	Training	10	15	4	5	-	1
	Trainees	2052	1511	1812	2022	-	2
2022	Training	23	13	6	7	-	5
	Trainees	1922	869	1612	2585	-	18
2023	Training	31	9	8	7	-	4
	Trainees	2652	979	964	1687	-	65
2024	Training	6	18	5	6	1	4
	Trainees	280	1360	1500	2443	33	74
2025**	Training	3	6	8	7	1	5
	Trainees	185	944	674	2440	10	81
Total	**Training**	**73**	**61**	**31**	**31**	**2**	**19**
	Trainees	**7091**	**5693**	**6562**	**11174**	**43**	**240**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

545. LEAs have developed several TF risks indicators as part of the collaborative process conducted under the Threat and Vulnerabilities working group, to help all enforcement agencies to detect and disrupt TF activities. These efforts are complemented by a range of guidance documents, prepared in accordance with their respective roles and responsibilities, covering a wide spectrum of TF typologies identified in Türkiye as well as best practices for disrupting and investigating them. For example, the TNP 2021, 2023 and 2025 "Guide on Combatting the Financing of Terrorism", the 2023 "Questions on Terrorism Financing Investigations and Statement Interrogation" and the 2024 "Evaluation of Alternative Money Transfer Methods and Virtual Asset Service Providers in terms of Terrorism Financing (Hawala)", among others, and the GGC 2021 and 2025 "Guidance On Effective Fight Against Terrorist Financing", "Countering Financing of Terrorism", and "Guidance About Informal Value Transfer Systems (Hawala)" as well as a control form (Hawala Control Form) to increase awareness of the personnel on their intranet web service, among others. MASAK also provides LEAs with up-to-date TF typologies guidelines, which includes recent trends, typologies and case examples to increase LEAs staff awareness of recent developments and provides indicators to be considered in the context of an investigation.

546. Operational detection capacity is strong and benefits from extensive data integration. Through UYAP, public prosecutors handling TF investigations can access in a single platform a wide range of information including bank account and transaction data, travel information and criminal-justice records. This allows prosecutors and LEAs to rapidly cross-check by combining financial footprints, travel, communications and criminal-justice records. These capabilities, supported by a widespread use of special investigative techniques, are a major operational strength.

547. Between 2021 and 2025 (Nov), Türkiye investigated a total of 11 476 TF cases and 23 349 natural persons were subject to TF investigations. While 47% of the total cases under investigation are related to ISIL/AQ financing, 24% related to PKK/KCK-PYD/YPG, 23% related to FETÖ, only 3% are related to other terrorist organisations.

548. In addition, Türkiye investigated a total of 421 216 cases and 376 978 persons for either leadership to an armed terrorist organisation, membership to an armed terrorist organisation and the provision of weapons to an armed terrorist organisation.

Table 9.3. Number of TF investigations (2021-2025)*

TO	2021		2022		2023		2024		2025**	
Terrorist financing offence (Law no.6415 Art.4/1)										
	No. investigations	No. Suspects	No. investigations	No. Suspects	No. investigations	No. Suspects	No. investigations	No. Suspects	No. investigations	No. Suspects
ISIL/AQ	741	1505	807	1105	844	1054	1253	1669	1746	1815
PKK/KCK-PYD/YPG	350	928	427	931	482	2720	719	3010	770	2697
FETO	241	569	269	573	333	575	472	1495	1358	1831
DHKP-C	7	43	82	89	58	154	236	181	63	75
Other	21	44	44	69	32	49	54	84	67	84
Total	**1360**	**3089**	**1629**	**2767**	**1749**	**4552**	**2734**	**6439**	**4004**	**6502**
Terrorism (TCL, Arts. 314/1, 314/2 and 315)										
Leadership to an armed terrorist organisation (TCL Article 314/1)	1783	1739	1985	1727	445	419	559	501	262	216
Membership to an armed terrorist organisation (TCL Article 314/2)	139343	113434	99934	84490	66865	60719	57075	63593	52686	49808
Providing weapons to an armed terrorist organisation (TCL 315)	75	76	67	83	80	88	31	52	26	33
Total	**141201**	**115249**	**101986**	**86300**	**67390**	**61226**	**57665**	**64146**	**52974**	**50057**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

549. The scale of investigations is significant and broadly reflects Türkiye's high exposure to TF risks, which involve the potential misuse of a wide range of financial and non-financial sectors. However, the volume of cases is not, in itself, determinative of effectiveness under IO.9, as it may be influenced by a high number of lower-value cases. At the same time, the demonstrated casework does not fully cover the full range of relevant TF risks, including areas where no ex-officio investigations were demonstrated.

550. Türkiye demonstrates a good ability to investigate TF offences related to UNSCR-listed and domestically designated terrorism threats in alignment with the country's risk profile. However, a significant effectiveness gap remains regarding TOs and networks not subject to designation under UNSCRs or Türkiye's domestic regime but identified through international sources and co-operation channels as relevant to Türkiye's TF risk exposure. In the context of its NRA, Türkiye has acknowledged that its TF risks are also shaped by its geographical position bordering areas of intensive instability and conflict. While Türkiye does not recognise certain regional actors as TOs, specifically those that are neither listed under the UNSCRs nor domestically designated, the risks stemming from those actors are described as being sensitively monitored. Yet Türkiye has not identified foreign-linked TF activity stemming from such

organisations within its borders, and did not report proactive or standalone TF investigations, prosecutions, or convictions specifically targeting them, despite Türkiye's geographic position as a key regional transit and connectivity hub. In some instances, however, Türkiye responded constructively to international requests for information related to individuals associated with such entities (see Box 9.2 regarding the two cases which have been presented). This materially limits effectiveness, as it constrains Türkiye's demonstrated ability to identify and investigate TF activity across the full spectrum of its relevant TF risk profile.

551. Türkiye identifies and investigates a broad range of TF activities involving both legal and illegal sources of funds. Authorities have identified the use of informal value transfer systems, including hawala-type mechanisms, VAs and social media-based fundraising, as well as schemes involving the misuse of NPOs and commercial entities. These cases demonstrate an ability to detect and investigate different TF methods. Demonstrated casework involving more complex structures, including the use of legal persons and commercial arrangements, remains limited and is concentrated in a narrower subset of TF cases related to FETÖ.

552. Detection gaps remain in relation to certain areas of Türkiye's TF risk environment. In particular, further demonstration is needed for cases involving TBTF, large-scale procurement activities and more complex financial structures, including those involving legal persons. While a range of TF methods has been identified, these are not yet systematically reflected in operational casework across the full range of relevant TF risks, which limits the extent to which Türkiye demonstrates coverage of its overall TF risk profile.

9.1.2. Investigations identifying the specific role of terrorist financier

553. Türkiye has implemented a holistic approach to identify the role of a terrorist financier in TF investigations. Türkiye uses different techniques to create a detailed financial footprint by connecting financial traces with operational realities to accurately identify and attribute the financier's role.

554. Public prosecutors use both financial intelligence and forensic evidence collection methods to identify a person's role as a terrorist financier focusing on (i) the identification of financial traces: enabling a comprehensive analysis of financial flows and ownership structures, revealing the origin, movement, and destination of the funds (i.e., analysis of bank transfers, SWIFT records, VAs chain analysis, payments done through MVTS, exchange houses, legal persons involved, cross-border cash declarations and disclosures, etc.; (ii) transaction timing, amounts, and cyclical transfers analysis to help detect suspicious patterns, while cross-border tracing and cash declaration reviews provide insight into international movements and undeclared assets; (iii) combining financial analysis with operational intelligence to enhance data validation (i.e., data bases cross-check, social media and donation campaigns monitoring to reveal potential fundraising channels, and witness statements or confessions obtained during interrogations linked to organisational structures); and (iv) the integrated use of technical surveillance that helps identify communication roles (e.g., recruiters, logisticians).

555. Although PFIs are widely used to identify the role of the terrorist financier, and many cases demonstrate detailed analysis of the collection, movement and use of funds, establishing the ultimate end-use of funds remains inherently challenging, particularly in complex or cross-border cases. In a number of instances, investigations focus primarily on the movement of funds, without fully demonstrating the final use, hierarchical roles, facilitators abroad, or the upstream organisational structure. While this reflects common evidentiary challenges in TF investigations, the absence of complementary elements—such as broader network mapping or identification of higher-level facilitators—limits the overall evidentiary depth in some cases. In addition, some cases involve small amounts, short financial cycles or single intermediaries, suggesting that operational facilitators are detected but that investigations do not always expand to identify wider networks.

9.2. Prosecuting and convicting different types of TF

556. Türkiye prosecutes and convicts a broad range of TF activities, largely in line with its identified TF risk profile relating to designated terrorist organisations.

557. Türkiye has increased TF prosecutions since the previous MER 2019, from 1 913 cases in 2013–2017 to 2 524 cases in 2021–2025, of which approximately 10% involved legal persons. Nearly half of the prosecuted cases are related to ISIL/AQ (43%) and the rest are related to domestic designated organisations PKK/KCK-PYD/YPG (26%), FETÖ (22%) and DHKP-C (6%) in line with the country's risk profile relating to designated TOs. Türkiye did not present prosecutions relating to cases linked to terrorist organisations or networks that are neither listed under UNSCRs nor designated at the domestic level but relevant to Türkiye's TF risk exposure. The majority of prosecutions involved the use of banking channels (46%), followed by cash courier activities (25%), abuse of legal persons (13%) and licensed MVTS (6%) and hawala-type transfers (5%).[39]

Table 9.4. Number of TF prosecutions (2021-2025)*

	2021		2022		2023		2024		2025**	
TF offence (Law no.6415 Art.4/1)										
TO	**No. Prosecutions**	**No. Suspects**	**No. Prosecutions**	**No. Suspects**	**No. Prosecutions**	**No. Suspects**	**No. Prosecutions**	**No. Suspects**	**No. Prosecutions**	**No. Suspects**
ISIL/AQ	73	155	206	320	204	313	245	405	366	605
PKK/KCK-PYD/YPG	187	318	142	205	93	186	125	179	116	194
FETO	110	235	72	145	124	350	107	147	135	389
DHKP-C	1	1	18	27	31	34	69	69	39	99
Other	10	22	18	36	12	32	7	14	14	17
Total	**381**	**731**	**456**	**733**	**464**	**915**	**553**	**814**	**670**	**1304**
Terrorism (TCL, Arts. 314/1, 314/2 and 315)										
Leadership to an armed terrorist organisation	448	563	567	669	113	156	92	117	59	56
Membership to an armed terrorist organisation	24 279	28 392	16 291	19 013	10060	13127	7806	9557	5311	6902
Providing weapons to an armed terrorist organisation	23	45	15	34	15	24	4	9	9	24
Total	**24750**	**29000**	**16873**	**19716**	**10188**	**13307**	**7902**	**9683**	**5379**	**6982**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

558. When a TF offence is evident alongside other terrorism-related crimes, such as membership in a terrorist organisation or providing arms or support, the public prosecutor determines the charges to be brought before the court. TF offences may be, and in practice have been, prosecuted concurrently with other terrorism-related offences, and it is ultimately for the judge to decide which charge aligns best with the evidence.

559. In cases where the TF offence can be coupled with membership, leadership or provision of weapons to an armed TO, the principle of concurrent offences applies, covering situations where a perpetrator meets the criteria for multiple penal provisions. Where evidence supports both TF and predicate terrorism

[39] Türkiye analyses MVTS and Hawala as two different concepts for statistics purposes. Due to the methodology applied, a single case may fall under more than one sector and/or typology of abuse.

offences, courts tend to prioritise terrorism-related charges, which carry heavier penalties than TF alone (see analysis under section 9.4). In such cases, TF conduct is often used as corroborative evidence of terrorist organisation membership.

560. Türkiye has substantially increased TF convictions since the previous MER, from 53 cases in 2013-2017 to 418 cases in 2021-2025[40], almost an eightfold increase, with 52% related to PKK/KCK-PYD/YPG, 32% to ISIL/AQ, 10% to FETÖ and 2% to DHKP-C and others. These convictions resulted in 584 convicted persons, the vast majority of whom were Turkish nationals (547). In line with the TF risk profile in relation to designated TOs, 49% of convicted persons were linked to PKK/KCK-PYD/YPG and 32% to ISIL/AQ.

Table 9.5. Number of TF convictions (2021-2025)*

	2021		2022		2023		2024		2025**	
TF offence (Law no.6415 Art.4/1)										
TO	**Convictions**	**Convicted persons**	**Conviction**	**Convicted persons**	**Conviction**	**Convicted persons**	**Conviction**	**Convicted persons**	**Conviction**	**Convicted persons**
ISIL/AQ	5	20	13	18	38	51	39	52	43	47
PKK/KCK-PYD/YPG	16	24	129	132	42	51	19	46	20	33
FETO	5	13	4	4	9	10	15	50	11	23
DHKP-C	0	0	0	0	3	3	0	0	1	1
Other	0	0	1	1	3	3	1	1	1	1
Total	**26**	**57**	**147**	**155**	**95**	**118**	**74**	**149**	**76**	**105**
Terrorism (TCL, Arts. 314/1, 314/2 and 315)										
Leadership to an armed terrorist organisation	99	109	67	75	56	60	43	50	37	36
Membership to an armed terrorist organisation	19241	22803	13541	16143	9465	11110	6919	8128	6637	7570
Providing weapons to an armed terrorist organisation	39	47	25	42	24	38	10	13	8	8
Total	**19379**	**22959**	**13633**	**16260**	**9545**	**11208**	**6972**	**8191**	**6682**	**7614**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025).

561. Türkiye has demonstrated the ability to prosecute and convict a wide range of TF activities. Approximately 90% of TF convictions relate to the provision of funds to terrorist organisations, predominantly PKK/KCK-PYD/YPG (57%), ISIL/AQ (28%) and FETÖ (13%). In contrast, the collection and use of funds account for a smaller proportion of convictions (10%), with nearly 60% linked to ISIL/AQ and 21% to PKK/KCK-PYD/YPG. This suggests that authorities are more effective in cases with a clear and direct nexus to a TO, while more complex TF typologies are prosecuted less frequently. The majority of convictions (76%) involved domestic fund movements, with the remaining 24% involving cross-border transactions.

562. Competent authorities acknowledge that a key challenge in securing TF convictions lies in establishing the requisite *mens rea*, particularly where funds are raised through small-scale, unauthorised social media campaigns presented as charitable causes, and where transaction amounts are low. In such cases, prosecutors rely on circumstantial evidence to demonstrate terrorist intent. Between 2021 and 2025 (Nov), Türkiye identified 59 cases in which prosecutions were initially initiated under TF offences but ultimately resulted in convictions for membership in an armed TO. Occasionally, these outcomes stemmed from a deliberate strategy by prosecutors, whereas in other instances they arose from pursuing alternative offences to achieve greater penalties.

[40] 2025 figures reflect information available up to the end of the on-site visit (November 2025).

563. While TF activity is subject to significant prosecution and conviction efforts, case studies and statistics point to uneven outcomes across the full risk profile. In particular, outcomes are less clearly demonstrated for TBTF, procurement networks, complex legal person structures, foreign-created legal persons and foreign legal arrangements, and TF activity linked to relevant non-designated terrorist organisations or networks. This is an important limitation in effectiveness, notwithstanding the high number of investigations, prosecutions and convictions overall.

9.3. Effectiveness, proportionality and dissuasiveness of sanctions

564. Türkiye has a robust sanctioning framework for natural persons convicted of TF, with imprisonment of 5-10 years for TF and 10-30 years when linked to organisational leadership, which is considered effective, proportionate and dissuasive. The absence of criminal liability for legal persons may limit Türkiye's ability to dissuade the misuse of legal persons for TF purposes.

565. TF is convicted either as a standalone offence or as an aggravating factor, increasing sentences by up to one-half. In practice, standalone TF convictions commonly result in around 4 years and 6 months; combined with other factors sentencing can reach up to 15–20 years with multiple aggravating factors. While combined TF with membership cases generally lead to 6–9 years. The minimum sentencing range for TF cases represents at least 2-5 times higher than for other serious crimes (i.e., 6 months for intentional damage to environment, 12 months for fraud, 3 years for tampering with a public tenders and aggravated theft) which is considered proportionate in Türkiye's context. TF sanctions (minimum 5 years) are aligned with terrorism-membership penalties and are generally harsher than standard economic crimes. Recidivism statistics (8% for 6415 offenders) also indicate a dissuasive effect. The substantial minimum sentencing range of 5 years, combined with the demonstrated willingness of courts to impose sentences of 6–20 years in aggravated cases, creates a credible deterrence signal for potential offenders, particularly given the public nature of conviction outcomes in high-profile FETÖ and ISIL-related cases.

Table 9.6. Sentencing range (2021-2025)*

TF standalone convictions				
Year	Minimum imprisonment range (days)	Maximum imprisonment range (days)	Average sentencing range (days)	Average sentencing range (years)
2021	755	2375	1637	4 years, 6 months
2022	755	2920	1773	4 years, 10 months
2023	755	2920	1609	4 years, 5 months
2024	755	2280	1586	4 years, 4 months
2025**	755	2190	1557	4 years, 3 months
Total average	**755**	**2537**	**1632**	**4 years, 6 months**
TF convictions coupled with membership, leadership or provision of weapons				
Year	Minimum imprisonment range (days)	Maximum imprisonment range (days)	Average sentencing range (days)	Average sentencing range (years)
2021	NIP***	NIP	NIP	NIP
2022	NIP	NIP	NIP	NIP
2023	1000	5840	3060	8 years, 5 months
2024	1140	3987	2374	6 years, 5 months
2025**	1520	3040	2469	6 years, 10 months
Total average	**1220**	**4289**	**2643**	**7 years, 3 months**

Note: (*) Data for 2020 were unavailable and are not reflected in the table; (**) 2025 figures reflect information available up to the end of the on-site visit (November 2025); (***) NIP: No information provided.

566. Sentences may be reduced by one-sixth upon judges' consideration or as part of the prosecutorial strategy. Defendants co-operating with authorities during the investigation/prosecution stage may receive discretionary reductions, and behaviour such as demonstrating remorse may also be considered. Although sentences can be reduced to 2–4 years, the sanctions remain proportionate and dissuasive in TF cases related to domestically and UNSC-listed terrorist organisations with a domestic nexus.

567. In line with Türkiye's fundamental principles of domestic law, legal persons are not subject to criminal liability for TF. Alternative measures, including confiscation and administrative sanctions, are available and have been applied in practice. Türkiye has demonstrated some cases involving the use of legal persons and commercial structures across different terrorist organisations. These examples show the ability to identify and take action against TF activity involving businesses. However, such cases remain relatively limited in scope and are not yet representative of consistent outcomes involving complex or layered structures across the broader TF risk environment. More developed and systematic casework involving legal persons is primarily observed in FETÖ-related commercial structures. Overall, the use of available measures remains relatively limited and does not yet demonstrate consistent outcomes involving complex or layered legal persons, legal arrangements and commercial structures across Türkiye's broader TF risk environment. The overall dissuasive effect of these measures is therefore not fully demonstrated, particularly given their materiality in Türkiye's economy and TF risk profile.

9.4. National counter-terrorism strategies and activities

568. Türkiye has a well-developed domestic CT/CFT strategy, with structured inter-agency mechanisms and policy documents. TF investigations, prosecutions and convictions inform the broader national CT Strategy and operational priorities, including typologies such as VAs, hawala, and the use of digital platforms for TF purposes. The National Security Council (MGK) and the National Security Policy Document (MGSB) set high-level threat perceptions, including PKK/KCK-PYD/YPG, FETÖ, ISIL and AQ. The Strategy Document on CFT, the Strategy Document 2021–2025 and the 2025 NRA provide a comprehensive framework for TF risk management, albeit with strong limitations where risks linked to non-UNSC and non-domestically designated organisations are assessed as not significant without detailed analysis. Competent authorities also analyse TF cases and update typology guides, STR guidance and sector-specific instructions.

9.4.1. Formulating national counter-terrorism strategies and activities

569. Türkiye demonstrates that TF investigations, prosecutions and convictions directly inform the formulation and updating of national CT/CFT strategies, through a structured bottom-up mechanism. Operational findings are systematically channelled into strategic documents, including the AML/CFT Strategy, the TF NRA, and the Strategy Document on CFT.

570. The core analytical contribution stems from the integration of operational casework into strategic decision-making. Türkiye provided multiple examples demonstrating that empirical findings from TF cases trigger concrete strategic adjustments, including:

a) reclassification of sectors (e.g. jewellery sector upgraded to high-risk following its use as a financial conduit in ISIL-related cases)
b) identification of emerging high-risk areas (e.g. VASPs, based on cases involving privacy coins and cross-border wallet structures)
c) introduction of regulatory measures (e.g. MASAK Communiqué No. 29 imposing enhanced due diligence and stablecoin restrictions)

d) expansion of the scope of obliged entities (e.g. inclusion of e-commerce platforms following TF abuse cases linked to FETÖ); and

e) prioritisation of cross-border risks and designation proposals, informed by international co-operation and financial intelligence.

571. In addition, typology development and guidance updates are derived from case outcomes, including the TF Typology Guide, sector-specific guidelines, and STR indicators. These outputs are regularly updated (most recently in 2025) and disseminated across competent authorities. These elements indicate that Türkiye effectively incorporates operational lessons into strategic frameworks, ensuring that national CT/CFT strategies remain responsive to evolving TF risks.

9.4.2. Sharing and using information and intelligence to support national counter-terrorism purposes and activities

572. TF investigation outputs are embedded in domestic CT/CFT strategies, supported by interagency co-ordination (e.g., Threat WG) and data integration into the NRA. The findings derived from investigations, prosecutions, and sentencing in TF-related cases constitute an important foundation for shaping Türkiye's TF and broader CT strategies and action plans.

573. Investigations, prosecutions and convictions outputs also inform the ongoing development and refinement of TF risk assessments and operational measures. For example, the Strategy Document, as a high-level policy instrument, addresses TF within a comprehensive framework through macro-level evaluations, while complementary documents such as the NRA provide more granular, sector-specific and organisational analyses by integrating risk factor assessments into operational planning. In addition, the Activity Report prepared in accordance with the Strategy Document is submitted to the Presidency of Türkiye Council for Legal Policies and the Presidency of Türkiye Security and Foreign Policy Council and serves as the basis for the MGSB outputs created under the MGK, as described earlier. In addition, the NRA is also sent to the Presidency of Türkiye General Directorate of Security Affairs and is therefore submitted to the President of Türkiye, who is the highest authority determining the country's CT strategies. Consequently, the mechanism described above, which feeds from the bottom up, serves as the basis for the policies of the Presidency of Türkiye.

574. However, evidence of how such information is systematically used for operational CT purposes (particularly for identification, targeting and designation of individuals and entities) is more limited. Although Türkiye reported examples of designation proposals submitted to the UN and the use of international co-operation (e.g. FIU exchanges, MLA, cross-border tracing), the link between TF case outputs and concrete CT actions is not consistently demonstrated. While information sharing mechanisms are in place and contribute to risk understanding and policy development, the extent to which TF intelligence is operationally leveraged for CT purposes, including designations and disruptions, is not sufficiently evidenced.

9.5. Alternative measures used where TF conviction is not possible (e.g. disruption)

575. Türkiye applies a range of alternative criminal justice and administrative measures in cases where securing a TF conviction is not practicable. These include the use of alternative terrorism-related offences, offences related to unauthorised payment services, deportation measures, administrative asset freezing, and transaction postponements. While this provides an additional avenue to address unlawful conduct, the available information does not clearly distinguish between preventive and alternative measures, nor does it sufficiently demonstrate their contribution to disrupting the financial aspects of TF activity.

576. Between 2021 and 2025 (Nov), Türkiye secured 59 convictions under alternative terrorism-related offences. This indicates that authorities are able to pursue alternative legal avenues where TF charges cannot be substantiated. In situations where the intent required for a TF offence cannot be established, authorities may pursue charges related to conducting payment services without proper authorisation. These measures can address illicit financial activity and may contribute to limiting the movement of funds, although their specific role in disrupting TF networks is not clearly articulated.

577. Türkiye also applies deportation measures in cases involving foreign nationals suspected of involvement in terrorism or TF. Deportation may occur following conviction or be applied as a preventive measure on national security grounds. Over the assessment period, 15 524 deportations of foreign nationals were executed, although it is not specified how many of these relate directly to TF. While such measures may reduce immediate risks, their impact on the underlying financial aspects of TF activity is less evident.

578. Administrative tools include domestic asset freezing and transaction postponements. Transaction postponements (1 677 cases) are used as short-term preventive measures, allowing authorities additional time to conduct analysis and, where appropriate, pursue further investigative or judicial actions. These measures can support broader investigative processes, but on their own are temporary in nature. Authorities may also refer cases to tax authorities where financial irregularities are identified but do not meet the evidentiary threshold for TF prosecution. While this provides an additional avenue to address unlawful conduct, the connection between such measures and the disruption of TF activity is not clearly demonstrated.

Box 9.3. Alternative conviction where TF prosecution was not possible

The defendant Mr. M was investigated for conducting extensive domestic and international money transfers via the hawala system on behalf of a suspected armed TO. Communications were intercepted pursuant to Art. 135 of the CPC. Mr. M routed transfer-related communications through encrypted messaging applications and received commission on transactions. A search of his residence yielded digital materials, account passbooks in foreign names, Temporary Protection Identity Documents, passports, EUR 11 000 and USD 6 830 in cash. CBRT reporting confirmed high-volume transfers across his bank accounts.

Although charges were brought for membership in an armed TO, the court found insufficient evidence of an organic link to the organisation's hierarchical structure and acquitted Mr. M of that charge.

The court nonetheless found on the basis of intercepted communications, seized materials, witness statements, partial confessions and CBRT findings, that Mr. M had systematically conducted unauthorised fund transfers for commission while actively concealing his activities. He was convicted under Article 28/1 of Law No. 6493 and sentenced to 10 months imprisonment. The seized cash was confiscated.

The case demonstrates the use of alternative financial legislation as a fall back where a TF conviction cannot be secured, allowing courts to sanction conduct and confiscate assets linked to suspected terrorist financing activity.

10 Terrorist financing preventive measures and financial sanctions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.10. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 6 and 8 and elements of R.14, 15, 16, 26, 30, 31, 32, 35, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) With its current framework Türkiye has been able to implement TF related TFS without delay to some extent. The process takes place on an average of 2.5 days due to the time required for the UN listing decision to be transposed into domestic law. Turkish authorities can apply mitigating measures to address to some extent for the potential delay with regard domestic transposition. TFS pursuant to UNSCR 1267 and its successor resolutions are not immediately enforceable in Türkiye upon UN designation. The time required for the UN listing decision to be transposed into domestic law impedes Türkiye's ability to implement TFS without delay. If funds or assets related to newly designated persons or entities are identified in Türkiye, the MoTF can postpone the transactions on the targeted funds and assets for seven working days However, this mechanism has not been resorted to over the reporting period.

b) Türkiye proposed individuals to the UNSC 1267/1989 and 1988 Committees for designation, in line with its risk profile. Over the reporting period, Türkiye submitted proposals to the UNSC for the listing of a total of 32 individuals under relevant sanctions regimes, with 14 of those proposals being co-sponsored by a UNSC member with one leading to a UNSC listing .

c) Türkiye has a robust framework and process for listing individuals and entities to its domestic designation (pursuant to UNSCR 1373) list and actively resorts to this tool. Türkiye has made use of its domestic regime and adopted asset freezing measures, including following requests from foreign countries in line with its risk profile. This has resulted in the asset freezing of 1 377 natural persons and 87 legal entities, with 325 freezing related to UN designated terrorist organisations.

d) Türkiye has made use of its TF TFS framework to a large extent to mitigate its TF risks, resulting in the freezing of a wide range of funds (over EUR 113 M) and assets of significant value. While the vast majority of funds and assets frozen are related to domestic designated TOs, Türkiye has

demonstrated its ability to target assets of individuals and entities related to TOs, including UN designated terrorist organisations under both UNSCR 1267 and 1373 regimes.

e) Türkiye has classified 80 195 associations as NPOs, and excluded foundations from this scope, on the basis of their financial materiality and exposure to TF risk which is not fully in line with the FATF functional definition of NPOs. Türkiye's NPOs monitoring also covers ML which goes beyond the scope of the FATF Standards. However, in practice Türkiye's monitoring of NPOs follows a RBA and is mostly focused on their potential abuse for TF purposes. Even though Türkiye's framework also provides for measures applying to the entire sector that could potentially disrupt or discourage legitimate NPO activities, the AT did not receive evidence that those are resorted to in practice. In line with its risk profile, Türkiye has also identified several NPOs being abused for TF purposes and taken measures mitigating measures accordingly.

f) FIs and VASPs are generally aware of their TF TFS obligations and complying to a certain extent. DNFBPs have a lesser understanding of their TFS obligations. Supervisory activities are conducted, and some violations have been detected. MASAK conducts its monitoring of TFS obligations following a specific RBS programmes for TFS. High and medium risks entities have been supervised on their compliance with TFS obligations except for legal professions and accountants. Reporting entities representing a medium to low risk, which represent the vast majority of entities within each sector, have been monitored to a much lesser extent, as Türkiye is monitoring compliance with TF TFS obligations following a risk-based approach. This does not preclude those entities from being potentially abused for TF TFS circumvention to some extent.

Key Recommended Actions (KRAs)

Türkiye should:

u) Ensure new designations for TF TFS are systematically implemented without delay.

v) Strengthen DNFBPs' understanding and compliance with TF TFS obligations.

w) Expand its supervisory efforts on TF TFS compliance for reporting entities, especially to those in sectors presenting high or medium risk of abuse for TFS purposes and that, within this category, have never been subject to a dedicated TFS supervision programme.

Other Recommended Actions

Türkiye should:

a) Conduct further outreach activities to reporting entities, especially DNFBPs, on the need for the implementation of TFS decision without delays.

b) Review its classification of associations and foundations falling within the FATF definition. On that basis, it should review which NPOs are the most at risk of being abused for TF purposes and pursue its monitoring of high risk NPOs following a RBA.

Overall Conclusions on IO.10

Türkiye's framework for the implementation of TFS pursuant to UNSCR 1267 requires domestic transposition of the UN listing decisions. With its current framework Türkiye has been able to implement TF TFS without delay to some extent and can apply mitigating measures to address to some extent delay in domestic transposition. Türkiye has identified assets and frozen assets of one individual under the 1267 regime. In line with its risk profile, Türkiye has also proposed several individuals for designations to the UNSC. Türkiye has also made use of its TF TFS framework to a large extent to mitigate its TF risks, resulting in the freezing of a wide range of funds and assets of significant value. Freezing, both in terms of number of persons/entities and value of assets, relate mostly to domestic designated TOs and to some extent to UN designated terrorist organisations.

FIs have identified and frozen terrorist funds and other related assets, including those owned, controlled or held by individuals acting on behalf of designated entities. This is indicative of FIs understanding of their TFS obligations. Despite the existence of various notification mechanisms most reporting entities except for banks and VASPs, still rely on manual checks on designation lists, which can be less effective, particularly given Türkiye's active use of domestic designations. DNFBPs have a more limited understanding of their TF TFS obligations. Türkiye prioritises monitoring of high risk entities with regard TF TFS compliance. Overall, a limited number of reporting entities (both FIs and DNFBPs) have been monitored against compliance with TF TFS requirements, which is a concern in light of Türkiye's risk profile.

Türkiye does not fully identify NPOs in line with the FATF functional definition, leading to the inclusion/exclusion on some entities on the basis of their financial materiality rather than on the type of activity they conduct. Türkiye's NPOs monitoring also covers ML which goes beyond the scope of the FATF Standards. Nevertheless, in practice Türkiye's monitoring of NPOs follows a RBA and is mostly focused on their potential abuse for TF purposes. In line with its risk profile, Türkiye has also identified several NPOs being abused for TF purposes and taken measures mitigating measures accordingly.

Türkiye is rated as having a Moderate level of effectiveness for IO.10.

Immediate Outcome 10

10.1. Implementation of TF-related targeted financial sanctions (TFS) without delay

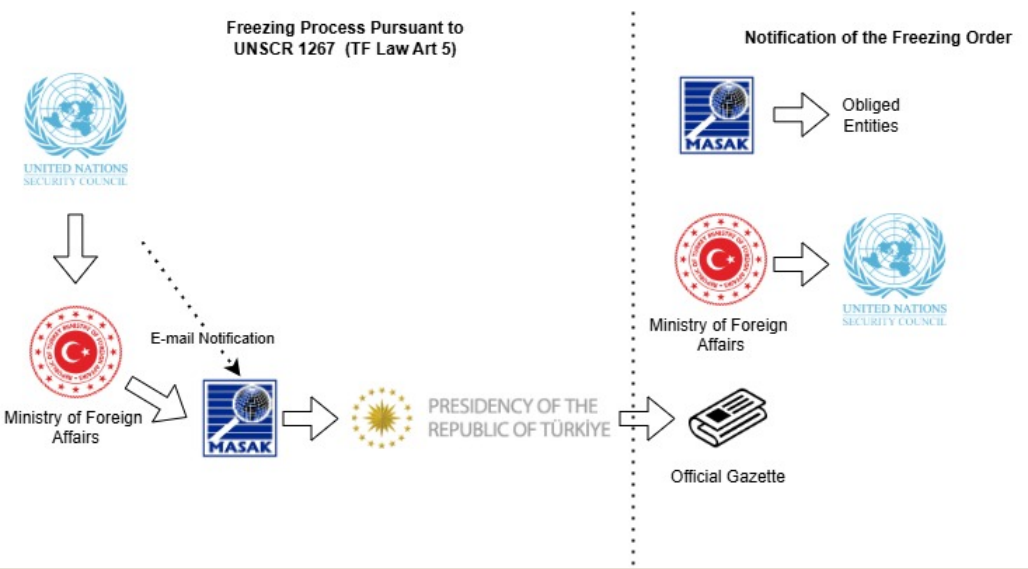
10.1.1. Designations pursuant to UNSCR 1267/1989 and 1988

579. TFS pursuant to UNSCR 1267 and its successor resolutions are not immediately enforceable in Türkiye upon UN designation. The process takes on average two and a half days for TFS to be enforceable in Türkiye, even though it represents a significant improvement from the estimated 33 transposition days in Türkiye 2019 MER, TF TFS related to UNSCRs 1267 and successors are not always implemented without delay.

580. When the UNSCRs 1267 and 1988 lists are updated, MASAK is notified without delay, both directly via the distribution list of the UN and via a formal letter from Türkiye's Permanent Representation at the UN. Upon receipt of the notification, MASAK notifies the Presidency of the Republic of Türkiye via a formal

letter signed by the MoTF to which a draft Presidential Decree is attached, this process also takes place without delay. Upon signature by the President of the Republic of Türkiye, the Presidential Decree is published in the Official Gazette and becomes enforceable. Since 2021, Türkiye has been able to implement this process without delay in some instances for TF TFS under the 1267 regime. Yet, the process takes place on an average of 2.5 days (see table below). The time required for the Presidential Decree to be formally signed is the main reason for the delay in the implementation.

Box 10.1. Infographic on TFS implementation



581. Türkiye can apply mitigating measures to address to some extent the delay in the legal enforcement of TFS under UNSCR 1267 regime. Prior to sending listings decision to the Presidency for ratification, MASAK identifies potential funds or assets and verify possible occurrences or links within Türkiye. If such funds or assets are found, the MoTF can postpone the transactions on the targeted funds and assets for seven working days (Law 5549, art. 19/A) even before the formal ratification of the Presidential decree implementing TFS would have occurred. However, as no matches were found over the reporting period, this mechanism has not been resorted to over the reporting period. This mechanism also relies on competent authorities' ability to identify potential funds or assets subject to UN freezing which can take time and would not automatically lead to the freezing of funds and assets by reporting entities without delay.

582. Türkiye proposes individuals or entities to the UNSC 1267/1989 and 1988 Committees for designation via Presidential Decree. The TFS Assessment Commission – chaired by MASAK and composed of relevant competent authorities (Presidency, National Intelligence, MoFA, MoI, MoJ, MoTF) – is the competent authority in charge to propose the names to President of the Republic of Türkiye. During the reporting period, five Presidential Decrees were issued in Türkiye, authorising the submission of proposals to the UNSC for the listing of a total of 32 individuals under relevant sanctions regimes, with 14 of those proposals being co-sponsored by a UNSC member, with one leading to a UNSC listing.[41]

[41] Türkiye submitted the proposal during the reporting period (2024), the UNSC designation occurred on 26 March 2026.

10.1.2. Designations pursuant to UNSCR 1373

583. Türkiye has a robust framework and process for listing individuals and entities to its domestic designation list and resorts to this tool to a large extent. The procedures and criteria for designation and de-listing are outlined in Law 6415 and are based on reasonable grounds that a person or entity has committed TF related acts (see Rec 6). Within this framework, MASAK is in charge of preparing a report based on its own intelligence or collected by other LEAs. The report is reviewed by the TFS Assessment Commission which is the authority in charge of proposing domestic listings that have to be co-signed by the MoTF and the MoJ. Once the decision is issued in the Official Gazette, it is immediately enforced and submitted, within 48 hours, to the Ankara High Criminal Court for judicial approval. The court reviews the decision in terms of the existence of reasonable grounds and must issue a ruling within five days, either upholding or revoking the asset freezing measure.

584. The Assessment Commission is responsible for reassessing the existence of reasonable grounds at intervals not exceeding six 6 months and submits its recommendation to the relevant ministers. In addition, relevant parties may request the lifting of an asset freezing decision. These requests are reviewed by the Commission and its recommendations are submitted to the Ministers. If the request is deemed unjustified, it is forwarded to the competent court for a decision on whether to maintain or lift the asset freezing measure.

585. Over the reporting period, Türkiye has made use of its domestic regime and adopted asset freezing measures following requests from foreign countries in line with its risk profile. Between 2021 and June 2025, under Türkiye's domestic freezing mechanism, a total of 19 Presidential Decrees were issued, resulting in the asset freezing of 1 377 natural persons and 87 legal entities, with 325 freezing related to UN designated terrorist organisations.

586. Asset freezing requests received from foreign countries are also evaluated by the Assessment Commission but finalised by Presidential Decree. In this framework, countries having information regarding targets that might meet the designation threshold (reasonable grounds) submit their request. MASAK prepares a report on this case enriched by relevant information from its own data sources and other relevant competent authorities. This report is then submitted to the Assessment Commission which can propose adoption of listing measures to the Presidency.

587. Among those 1 434 assets freezing decisions, 62 individuals and 8 legal entities had their assets frozen in Türkiye following requests submitted by two foreign countries. As for rejected foreign requests, the average response time for notification to the relevant country is 8 months. Situations requiring additional information to be provided by the requesting country, may lead to an extension of the evaluation period.

Box 10.2. Joint designations with a foreign country

Within the framework of the joint mechanism established with the US to prevent the TF, five individuals and two legal entities have been identified for transferring funds to ISIL members and their families. The assets of the individuals and legal entities were frozen simultaneously in 2023 (1). Subsequently, five individuals whose assets were frozen as a result of denunciation were convicted of TF offences, while a confiscation order was issued against one legal entity.

In 2023 (2), the assets of two other individuals alleged to have facilitated ISIL financing activities in conflict zones were frozen as part of joint efforts with the US and an indictment was issued against one of the individuals for TF offences.

In 2024 (3), the assets of three foreign individuals alleged to have carried out educational and logistical activities in Türkiye were frozen. These individuals were found to have links to those who carried out the 2024 attack on a church in Sarıyer. Criminal denunciations were filed against the three individuals and two of them have been convicted of membership in a terrorist organization, while one had been acquitted of the same charge.

Source:

(1) https://home.treasury.gov/news/press-releases/jy1181

(2) https://home.treasury.gov/news/press-releases/jy1456

(3) https://home.treasury.gov/news/press-releases/jy2406

588. Designations are published in the Official Gazette and by law MASAK has to inform competent authorities as well as natural and legal persons to whom notification is deemed necessary. Decisions are communicated on MASAK website and via an e-notification system with banks and most financial institutions. Clear guidance to FIs and other persons or entities, including DNFBPs that may be holding targeted funds or other assets, on their obligations to take freezing action is also available on MASAK website.

589. In order to immediately block any potential financial activity following an asset-freezing decision updates in the lists are securely shared with FIs several hours prior to publication in the Official Gazette. Upon issuance of the freezing order, all bank accounts, debit and credit cards, e-money accounts, and virtual assets belonging to the designated individuals have to be blocked.

590. Natural and legal persons, as well as public institutions and organisations, are required to inform MASAK of any "asset records" within 7 days, upon the notification of the freezing decision. In practice, this delay could impede competent authorities to become aware of the frozen assets in a timely manner and take appropriate actions. In addition, designated individuals and entities are required to inform MASAK of all other assets, and natural and legal persons who are in claim or debt relationship with those about whom decision on freezing of asset has been made and shall also inform MASAK of the amount of the claim or debt within 30 days of publication of the freezing decision. This has happened in practice in relation to the individuals listed under the UNSC 1267/1988 regime and whose assets have been identified and frozen in Türkiye.

10.2. Identification and deprivation of terrorist funds or other assets

591. Türkiye has made use of its TF TFS framework to a large extent to mitigate its TF risks. Over the reporting period, under Türkiye's domestic freezing mechanism, 1 377 natural persons and 87 legal entities

have been subject to asset freezing. Out of those 1 434 assets freezing decisions, 1 109 were related to domestically designated organisations and 325 to UN designated terrorist organisations. While 88% of the listed persons are Turkish nationals, Türkiye has citizens from more than 25 countries on its domestic list which is in line with the country risk profile. Also, 62 individuals and 8 legal entities were subject to assess freezing measures in Türkiye following requests submitted by two foreign countries.

592. Due to the entry into force of the TFS mechanism in December 2020, 1 145 natural persons were listed in 2021. Since, Türkiye has on average listed 58 individuals and 18 entities yearly since 2022. Overall, 15 decisions were lifted through formal legal procedures, with the Court considering as insufficient the "reasonable grounds" supporting the freezing decision. A significant portion of the designated individuals are Turkish nationals, with several foreign individuals from abroad. Türkiye has made use of its domestic regime to also freeze assets of persons/entities acting on behalf of designated persons.

593. Authorities monitor financial activities of close relatives and commercial associates of designated individuals. If suspicious fund transfers linked to a designated person are detected, the relevant transaction is suspended with Ministerial approval and if there is enough evidence, the matter is also referred to the PPO. Where justified, such entities or individuals are also subjected to asset-freezing measures.

Box 10.3. Use of TF TFS mechanism against terrorists or persons acting on their behalf

Case study 1: As a result of investigations into preventing ISIL financing, in April 2021, the assets of an individual named S.Ö. were frozen. During monitoring activities, intelligence information was received from TNP that informed MASAK about the accounts of S.Ö.'s sister, F.Ö., which had previously been rarely used, showed a significant volume of transactions after the freezing decision. Upon this, F.Ö.'s accounts were examined, and it was observed that some of the transfers were made to individuals who had previously been subject to legal proceedings within the scope of ISIL, and that some of the transactions matched to the TO's fundraising methods. Consequently, a report was prepared on F.Ö., and the individual's assets were frozen in June 2022.

Case study 2: During the investigation into T.K., whose assets were frozen in January 2025 regarding his affiliation to ISIL, intelligence later confirmed by a bank STR indicated that he used accounts opened in the name of his mother, G.K. After T.K.'s assets were frozen, an investigation into his mother G.K.'s accounts revealed unusual transactions in one of the individual's accounts starting the day after the aforementioned decision. The relevant bank was contacted to take the necessary measures. As a result, the individual's accounts were frozen.

Case Study 3: In January 2022, a domestic VASP reported suspicious activity concerning two users, whose names appeared in adverse media alleging ISIL involvement as regional logistics operatives. Key findings from the investigation included: VAs deposits and withdrawals linked to small foreign platforms, other suspicious users transacting with the same wallet addresses, and arrests of both individuals in 2019 for suspected ISIL ties MASAK's deeper review revealed that the terminology used in transactions was consistent with ISIL donation language, the financial behaviour inconsistent with declared income levels, Tether USD (USDT) transfers made to multiple wallet addresses, evasive responses in compliance-related communications with VAs firms. In June 2022, asset-freezing orders were issued for three individuals who had transacted with the same wallets. In addition, criminal complaints were filed, and judicial proceedings are still ongoing.

594. Türkiye's efforts to identify assets have resulted in the freezing of accounts and assets, including movable and immovables ones, not only owned directly by designated individuals, but those that are controlled by the designated individual. These are accounts or assets belonging to the spouse or other relatives of the designated persons and entities that have been used to circumvent the asset freezing

decision. The AT did not find evidence that the mechanism was being used to disproportionately target all funds and assets of relatives of designated persons and entities.

Table 10.1. Assets frozen related to TF TFS

Sanctions Regime	Affiliated organisation	Value EUR	Real Estate	Motor Vehicles	Gold (g) & Jewelry	Legal persons
UNSCR 1267/1988	UN designated terrorist organisation	1 200	-	-	-	-
UNSCR 1373	FETÖ	112 122 710	851	66 + 1 yacht	107g + 76 precious items	132
	PKK-KCK	921 953	303	8	-	-
	Leftist organisation	102 230	103	3 + 1 yacht	-	8
	ISIL & Al Qaeda	568 560	283	49	11g	31
UNSCR 1373 (upon foreign requests)	ISIL & Al Qaeda	23 120	1	9		5
Total	-	113 739 773	1 541	137	118g + 76 precious items	176

595. To prevent designated individuals and entities from receiving funds through indirect means, MASAK regularly reviews reports submitted by FIs either based on detected links or through their own risk assessments. This process ensures that no financial support is channelled to listed persons via proxy individuals or organizations.

596. MASAK manages the requests for access to funds and assets that are frozen following the procedures set out in UNSCR 1452. The designated persons shall notify all their rights, receivables and payables and other assets to MASAK electronically and in writing within thirty days as from the date of publication of the asset freezing decision the process, by filling out forms available MASAK's website. Between 2021 and November, 2025, Türkiye received 118 requests for access to frozen assets out of which 77 permissions to access frozen assets were granted.

10.3. Targeted application of focused and proportionate mitigation measures to at-risk non-profit organisations

597. Türkiye has classified 80 195 associations as NPOs, on the basis of their financial materiality and exposure to TF risk which is not fully in line with the FATF functional definition of NPOs. As of July 2025, the non-profit sector in Türkiye consisted of 101 237 associations and approximately 6 400 foundations. Authorities have classified associations in 22 subgroups, out of which Türkiye considered that 80 195 fall within the FATF definition of NPOs on the basis that their subgroups account for more than 1% of total financial activity of the NPO sector. As a result of these calculations, 16 subgroups[42] have been considered to fall within the FATF definition of NPO. Türkiye also excluded 6 subgroups from the FATF definition of

[42] Associations for: 1) Professional and Solidarity Associations (social) ,2) Sports and Sports-Related Associations (social and cultural) , 3) Associations Engaged in Activities Related to the Provision of Religious Services (religious), 4) Education Research Associations (education), 5) Culture, Arts, and Tourism Associations (cultural), 6) Humanitarian Aid Associations (charitable), 7) Associations for Preserving Social Values (cultural), 8) Associations Engaged in Health Activities (good works), 9) Urban Planning, Development, and Improvement Associations (good works), 10) International Organizations and Co-operation Associations (good works), 11) Environmental, Natural Life, and Animal Protection Associations (good works), 12) Associations for the Disabled (good works), 13) Associations Active in the Fields of Food, Agriculture, and Animal Husbandry (good works), 14) Associations for Solidarity with Turks Abroad (good works), 15) Associations for the Elderly and Children (good works),16) Associations for Individual Education and Social Development (social).

NPOs (see R. 8). This approach is not fully in line with the FATF definition of NPOs which focuses on function (i.e. raising or disbursing funds) and some associations included in the scope of NPOs may have been excluded based on the types of activity they carry out and vice versa. Similarly, foundations, have been excluded from the scope of NPOs based on their low TF risks according to the results of the 2023 and 2025 NRA, and since entrance into the sector requires more rigid procedures.

Identification of at-risk NPOs

598. Türkiye's General Directorate of Relations with Civil Society (GDRCS), under the Ministry of Interior, is the competent authority responsible for monitoring NPOs. It maintains up-to-date information on NPOs via DERBIS. Türkiye's classification as NPOs on the basis of their financial materiality and TF risk exposure which is not fully in line with the functional definition of NPOs has on the other hand supported the oversight of NPOs to focus primarily on those most at risk of TF. Türkiye already takes into account a risk element when establishing the associations that fall under the definition of NPOs. In addition, the GDRCS conducts a yearly robust risk assessment to determine which NPOs are most at risks of being abused for TF purposes. Associations operating in Türkiye are divided according to their fields of activity (types) and an examination is made on which associations operating in which fields are at risk. Afterwards, an analysis of the current situation in institutional, economic, geographical and demographic frameworks was also conducted taking into account nine risk criteria.

599. Türkiye considers that the highest TF risk within the NPO sector is to be found within humanitarian aid associations operating close to an area posing an active terrorist threat such as the southern border, which is in line with the country's risk profile. Türkiye has conducted a thorough risk assessment of the sector and established a risk scoring methodology revised on a yearly basis, allowing to consider that only 1.2% of the NPO population represent a high or medium risk. The GDRCS re-evaluates yearly the risk ratings of high and medium risk NPOs. This has led to amending NPOs risk scores, especially downgrading the risk from high to medium risk or even from medium to low risk, thus being left out of the scope of monitoring/auditing process. As a result of risk analyses conducted within the scope of the methodology, a total of 1 095 associations changed risk groups between 2023, 2024 and 2025 which demonstrates that the methodology is actively working and effective. Over the reporting period a yearly average of 135 NPOs are considered high risk yearly, and 710 medium risks.

600. While the number of high risks NPOs has remained relatively stable, the number of medium risks NPOs varied more intensely, reflecting contextual factors. For instance, the number of medium risks NPOs has more than doubled between 2024 and 2025. This is explained as the determination of the risk scoring for NPOs in 2025 was based on the information available on NPOs as of the 2023 financial year. However, in 2023, Türkiye suffered from a massive earthquake, leading NPOs to receive much more funds from abroad than usual and deploy activities in the regions most affected, which are neighbouring Syria and represent a higher potential TF risk. This contextual factor explains the surge in the number of NPOs classified as medium risk in 2025.

Table 10.2. NPO risk classification (2021-2025)

Year	High risk NPOs	Medium risk NPOs
2021	170	1 172
2022	169	533
2023	115	558
2024	100	432
2025	131	860

NPO oversight

601. In Türkiye, NPOs in the form of associations are formed by at least seven natural or legal persons and acquire legal personality without the need for prior permission the moment they submit their establishment notification the local administrative authority. Foreign NPOs can engage in activities in Türkiye and open representative offices subject to approval from the MoI. NPOs information is centralised in DERBIS which both, authorities and NPOs, consider very convenient to keep up-to-date information.

602. Türkiye's legal framework provides for measures applicable to all NPOs which could unduly disrupt or discourage legitimate NPO activities. For example, all NPOs are obliged to submit a yearly financial statement, to report the aid they receive from abroad before using it, to report beforehand any aid they will be providing and all persons collecting aid should obtain prior authorisation from competent authorities. NPOs are also not only monitored in the scope of TF but also for ML purposes which goes beyond the requirement of the FATF Standards and could create unjustified additional oversight of NPOs activities.

603. Notwithstanding the above, the AT did not receive evidence that the mentioned measures are resorted to in practice to unduly disrupt NPOs activities. During onsite meetings, representatives from the NPO sector considered those measures as necessary, in light of Türkiye' specific risk exposure, to ensure the soundness of the NPO sector in the country and that those requirements facilitate the establishment of relationship with foreign donors. In addition, in January 2024 the Constitutional Court annulled the provision of the Law on Associations (Law 5253) that gave powers to the MoI to temporarily suspend the activities of an NPOs on the basis of a suspicion of a criminal activity. Authorities confirmed that they have no intention to reintroduce such measure.

604. Following a RBA, Türkiye has focused its oversight activities on the high and medium risk NPOs. In light of the yearly risk scoring described above, the GDRCS focuses its audit activities on all high risk NPOs yearly and medium risk NPOs at least every two years. Even though Türkiye's framework provides for the audit of low-risk NPOs, more than 80 000 entities, the GDRCS do not in practice conduct such audits as it is impossible to audit such a large population and oversight efforts are focused on the higher risk entities in line with a targeted, RBA. To support audit activities, Türkiye developed regulations and guidance for NPOs' oversight limiting the scope of the audit an NPO is subject to. Monitoring of NPOs is conducted by GDRCS within the framework of the risk-based audit methodology updated annually. All NPOs the AT engaged with during the onsite visit had been subject to onsite monitoring by GDRCS, none consider that the scope of the audit was too broad nor that it disrupted their activities. Some received fines which they considered helpful to improve further their compliance with the requirements.

Table 10.3. Outcomes of audits for high and medium risks NPOs (2021-2025)

Year	Audited Associations	Judicial Fine	Administrative Fine	Both Judicial Proceeding and Administrative Fine
2021	1 342	21	370	53
2022	701	23	273	43
2023	671	18	301	29
2024	530	11	189	18
2025*	560	9	243	29

Note: (*) Covering the period from 1 January - 28 November 2025

605. Sanctions against NPOs are applied in a proportionate manner depending on the degree of the offence. Fines and sanctions are defined by law following the principle of proportionality, hence limiting

the discretion of the administration. Also, sanctions, administrative fines or judicial fines/penalties are not to be imposed to the NPOs themselves in accordance with the principle of individual criminal responsibility, penalties can be only imposed to the natural person(s) who committed the misdemeanour or the crime. The most common reasons for imposing sanctions on NPOs as a result of monitoring activities are failure to notify and keep proper books obligations, such as failure to submit the association declaration, holding general assembly meetings, failure to comply with money transfer obligations through the banking system (including by resorting to hawala) or discrepancies with accounting procedures and principles.

606. In line with its risk profile, Türkiye has also identified several NPOs being abused for TF purposes and taken measures mitigating measures accordingly. GDRCS informs other relevant authorities in cases where an association is suspected to being linked to a TO or TF, GDRCS may either notify MASAK or it may directly report a criminal complaint to the public prosecutors. Türkiye has frozen the assets of 3 NPOs located in Türkiye, of whom 2 are considered to be affiliated to UN designated terrorist organisations. In addition, 35 NPOs located abroad have been added to Türkiye domestic listing regime, all are branches of NPOs linked with domestically designated TOs.

Box 10.4. NPO abused for TF purposes

Following an audit by the GDRCS, Association X was reported to MASAK for analysis due to various suspicions, including being used to finance activities and carry out propaganda in support of a domestically listed TO.

As a result of the analysis conducted by MASAK, it was found that many financial transactions were carried out within the scope of the domestic TO's financial structure, management and activities of the association were dedicated to the organisation. Front companies were also used to provide financial support to the organisation and conceal their activities. These front companies were connected to genuine commercial enterprises that could act as intermediaries in providing financial support to the organisation. Intelligence obtained from security and intelligence units also revealed that the funds collected were also used to finance experienced members of the terrorist organisation who issued orders for actions and activities within Türkiye, as well as to support terrorist acts.

A was sent to the Chief Public Prosecutor's Office to initiate legal proceedings. Accordingly, 23 suspects, including individuals identified as having been selected from among those holding managerial positions within the domestic terrorist organization, were investigated on charges of "membership in an armed terrorist organization" and "propaganda for a terrorist organization.

Following a thorough examination of the information and documents obtained from relevant institutions and organisations regarding data accessed by MASAK, it was assessed that the activities of the individuals subject to the analysis could constitute reasonable grounds for the commission of acts falling within the scope of the crime of terrorist financing. The Evaluation Commission recommended to the MoTF and the MoI that the assets of several individuals and Association X in Türkiye be frozen. Association X was then dissolved by decision of the Civil Court of First Instance in 2024.

607. Authorities have engaged with the sector to a large extent in awareness raising activities and demonstrated efforts to monitor the sector without disrupting legitimate activities especially for NPOs operating in high-risk areas. Authorities established several guidance and good practices paper to inform NPOs about their risks of being abused for TF purposes and have conducted many outreach activities to raise awareness in the sector, for over 50 000 NPOs representatives. The GDRCS is deployed in all 81 provinces in Türkiye and NPO oversight is achieved via the local governorate and association auditors which ensure close relationship and understanding of the realities NPOs face on the ground. NPOs representatives highlighted the close co-operation with the GDCRS. Some NPOs operating in high-risk

areas (i.e. at the border with Syria) and met during the onsite visit underscored the close co-ordination with the GDRCS for them to access the formal financial system to receive funds and also in the disbursement of their aid in cash if needed (e.g. where no bank presence).

10.4. FIs, VASPs and DNFBPs understanding of and compliance with obligations

10.4.1. FIs and VASPs

608. FIs and VASPs have a generally good understanding of their TF TFS obligations, including their obligation to freeze funds and other assets without delay. A guidance on TFS obligations for reporting entities was published in 2022 and competent authorities are in the process of updating it. Understanding of TFS obligations has also been supported via trainings and outreach activities.

609. FI and VASPs rely on international monitoring programs and apply daily screening to their customer database. In some instances, FIs have identified and frozen terrorist funds and other related assets, including those owned, controlled or held by individuals acting on behalf of designated entities. This is indicative of financial institutions understanding of their TFS obligations.

610. Smaller FIs, as well as capital markets institutions and NBFIs mostly rely on manual screening. Concerns arise in the timely implementation of TFS obligations for FIs and VASPs that do not use commercial databases that automatically update sanctions lists. While this is likely marginal for banks and VASPs, most other FIs rely on manual screening, the lack of systematic updates can cause delays in TFS compliance. In addition, exchange offices and MVTS interviewed by the AT during the onsite visit mostly screen customers at the onboarding stage but monitor their ongoing business relationship to a lesser extent which also creates concerns, especially in light of the exposure of those sectors to TF abuse.

10.4.2. DNFBPs

611. Apart from some entities, DNFBPs have in general a limited understanding of their TF TFS obligations, especially with regard the need to implement those obligations without delay. DPMS and REAs considered that the structure of their client relationship (mostly single transaction) exposes them to less risks in terms of TFS, while accountants and legal professions consider that having well-known databases of customers mitigate their risks. While DNFBPs are mostly aware that TFS lists can be consulted on MASAK website, there were shortcomings in the understanding of what TFS decisions relate to and the scope to whom those decisions would apply to, which is not limited to foreign individuals (some mentioned "foreigners"). Furthermore, most DNFBPs met during the onsite visit considered that their exposure to TFS risks was minimal as they perform transactions through the banking system, so the reliance on other reporting entities is seen as a major mitigator of their risk. This is a concern as it prevents sound implementation of TFS requirements.

612. DNFBPs only perform screening at the onboarding stage which is not in line with their TFS obligations. While direct notification process exists, most DNFBPs rely on manual checks of the UN and MASAK websites. Not all entities are aware nor subscribed to MASAK's notification system. This can create challenges in ensuring their sanctions databases are updated in a timely manner. The fact that no DNFBP has reported potential matches, despite Türkiye's active use of domestic designations, is a concern on the limited understanding and compliance of the sector with TF TFS obligations.

10.5. Competent authorities monitoring and ensuring compliance with TF-related targeted financial sanctions

10.5.1. FIs and VASPs

613. Türkiye is monitoring FIs and VASPs compliance on TF TFS to some extent. In line with its 2021 ICRG Action Plan, Türkiye implemented a risk-based approach for monitoring reporting entities compliance with TFS obligations, by developing separate supervision programmes based on a separate risk analysis specifically for TFS monitoring, both in terms of TF and PF. On an annual basis, competent authorities assess reporting entities risk level for TFS compliance taking into consideration several factors such as control measures applied by reporting entities, asset size, outcome of previous inspections. Within each sector, reporting entities are then categorised into high/medium and low TFS risk and authorities conduct onsite inspections to all high risks entities and some medium risks. Apart from planned inspections, if evidence emerges that an obligated party has violated the sanctions, that party is supervised independently of the program, and sanctions are imposed in case of violation. Periodic inquiries are also conducted to determine whether individuals and legal entities on asset freeze lists have committed any violations following the freeze decision.

614. As a result, between 2022 to 2024, Türkiye has inspected over 500 FIs, VASPs and DNFBPs on their compliance with TFS obligations, out of which all high risks entities from each sector have been monitored. Almost 300 FIs and VASPs have been inspected with 25 entities found to have been violating TFS obligations. No distinction has been provided to the assessment team on specific TF TFS obligations monitoring and violations. Compliance with those obligations has increased over the reporting period for financial institutions and VASPs that have been inspected. Cases where FIs violations have been identified by supervisors mostly relate to persons whose assets were frozen having multiple names or their names could be typed in various ways which lead the names not to match with the one used by the reporting entity. In cases where co-ordination between the compliance and operational units could be further strengthened, FIs receive a formal warning notification.

615. Despite having followed a RBA, over the reporting period Türkiye has only monitored compliance with TFS obligations for approximately 20% of FIs through dedicated supervision programmes which represents a limited portion of the entire sector. In addition, the amount of the sanctions applied for TFS violations is low and does not appear to be dissuasive nor proportionate.

Table 10.4. TFS supervisory actions

Sector	2022				2023				2024			
	High Medium risks	Supervised obliged entities	Number of obliged entities in violation	Fines (EUR *1 000)	High Medium risks	Supervised obliged entities	Number of obliged entities in violation	Fines (EUR*1 000)	High Medium risks	Supervised obliged entities	Number of obliged entities in violation	Fines (EUR*1 000)
Banks	17	17	4	181	21	16	5	190	33	16	1	2
Factoring / Leasing / Financing Companies	22	8	0	0	52	13	0	0	41	12	0	0
Capital Market Intermediaries	10	10	0	0	25	10	0	0	22	10	0	0
Portfolio management companies &	2	2	0	0	14	2	0	0	5	1	0	0

Sector	2022				2023				2024			
	High Medium risks	Supervised obliged entities	Number of obliged entities in violation	Fines (EUR *1 000)	High Medium risks	Supervised obliged entities	Number of obliged entities in violation	Fines (EUR*1 000)	High Medium risks	Supervised obliged entities	Number of obliged entities in violation	Fines (EUR*1 000)
Investment Partnerships												
Insurance Companies	11	8	4	6	26	8	2	6	33	8	0	0
MVTS	16	16	3	18	24	13	4	11	22	14	1	1
EOs	146	30	0	0	121	29	0	0	110	31	1	3
VASPs	--	-	-	-	25	10	0	0	23	10	0	0
FIs total	224	90	11	205	308	101	11	207	289	102	3	6
REAs	107	10	0	0	115	16	0	0	82	17	0	0
DPMS	200	55	0	0	216	51	0	0	241	58	1	114
DNFBPs total	307	65	0	0	331	67	0	0	323	75	1	114
Total	**531**	**155**	**11**	**205**	**639**	**168**	**11**	**207**	**612**	**177**	**4**	**120**

10.5.2. DNFBPs

616. As described above, authorities developed risk-based supervisory programmes to specifically monitor compliance with TFS obligations for reporting entities. For DNFBPs, those supervisory activities covered approximately 200 entities, including all high and some medium risks DPMS and real estate agents. Only one entity within the DPMS and REAs sector was found as violating its TF TFS obligations within the reporting period. This result does not fully align with the overall low level of understanding of TFS obligations across those sectors.

617. Overall, only a marginal portion of DNFBPs have been monitored against their TFS obligations, this finding coupled with the deficiencies in the understanding of TFS obligations, increase the risk of potential abuse of the DNFBP sector by designated persons or entities. There was no supervision of compliance with TFS obligations for accountants, lawyers and notaries. Given the shortcomings in TFS understanding of those sectors, the absence of supervision is concerning.

11 Proliferation financing financial sanctions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.11. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 7 and elements of R.1, 2 and 15.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Türkiye's competent authorities have a framework in place that ensures good co-operation and co-ordination in the implementation of policies for operational purposes on CPF, especially in developing measures to mitigate risks linked to trade and PF sanctions evasion. In particular, the country has a comprehensive export control framework on dual-use goods and technologies.

b) Türkiye has an overall good understanding of its PF risks supported by the recent publication of both a PF Strategy and NRA. It covers the financing of weapons of mass destruction (WMD) and also includes elements on potential breaches, non-implementation and evasion of PF TFS. Those documents also support the implementation of mitigating measures to some extent, but actions are still to be taken in light of their recent adoption. Risks related to potential sanctions evasions via the misuse of legal persons, including foreign ones, are understood to a lesser extent and could hinder Türkiye's ability to deter PF risks to some extent.

c) Türkiye has a mechanism to implement PF TFS. This mechanism is similar to the one implementing TF TFS which ensures application without delay, to some extent and not in a consistent manner as the process takes place on an average of 2.5 days. Communication mechanisms are identical to those described under IO.10 and support the implementation of PF related TFS (see IO.10).

d) Türkiye has been applying PF related TFS on DPRK and Iran since 2021 and has listed individuals and entities accordingly in line with relevant UNSCRs and the FATF Standards for the vast majority of the reporting period. However, as of the end of the onsite visit, individuals and entities listed in relation to UNSCR 1737 and successor resolutions were still listed in Türkiye within the scope of UNSCR 2231 which no longer provides for the implementation of TFS since the snapback mechanism to UNSCR 2231 entered into force on 27 September 2025.

e) Reporting entities' level of understanding and compliance with their PF related TFS is generally low. While banks comply with their obligations to a certain extent, there is a severe lack of

understanding of PF risks in the other sectors, coupled with challenges on the concept of beneficial owner (see IO.4), which impede reporting entities' ability to identify methods of evading PF TFS beyond list screening. Even though Türkiye monitored compliance with TFS obligations - indiscriminately on both TF and PF - for all high and some medium risk entities, it still represents an overall limited portion of reporting entities. The specific risks related to potential breaches and evasions of sanctions is not taken into consideration by most reporting entities.

Key Recommended Actions (KRAs)

Türkiye should:

x) Ensure it implements PF related TFS without delay.

y) Implement PF related TFS on Iran within the scope of UNSCR 1737 and its successor resolutions.

z) Strengthen reporting entities' understanding and compliance with PF related TFS.

Other Recommended Actions

Türkiye should:

a) Enhance its understanding of PF risks related to the potential misuse of legal persons, including foreign legal persons.

b) Monitor compliance with PF TFS for a larger scope of reporting entities, beyond the ones posing a high risk.

c) Conduct additional outreach activities to raise awareness of the DNFBP sector on PF related TFS.

Overall Conclusions on IO.11

Türkiye has several co-ordination bodies in relation to CPF and effectively co-operate and co-ordinate to design policies to combat financing of WMD. Those mechanisms supported setting up several recent policy objectives and documents. Their effective implementation is yet to be fully demonstrated due to their recent establishment. Overall, Türkiye's competent authorities demonstrate good co-operation and co-ordination for operational purposes in combatting the financing of weapons of mass destruction. Türkiye has established a comprehensive export control framework on dual-use goods and technologies, supported by the operational co-ordination of the various government institutions.

The understanding and update of PF risks has been set as a policy objective in Türkiye with the adoption of the PF Strategy Document (2025-2029). As a result, Türkiye completed its first PF NRA in 2025 which supported an enhanced understanding of PF risks, including in relation with evasion of PF related TFS.

Yet, understanding of circumvention of PF related TFS remains generic and could be further strengthened, especially potential sanction evasions via the misuse of legal persons. Implementation of mitigating measures is taking place to some extent but are not fully effective in light of their recent adoption.

Türkiye has a similar mechanism for the implementation of PF and TF TFS which ensures application without delay to some extent and not in a consistent manner (see IO.10). Türkiye has been applying PF related TFS on DPRK and Iran since 2021 and has listed individuals and entities accordingly in line with relevant UNSCRs and the FATF Standards for the vast majority of the reporting period. Türkiye had listed individuals and entities included in UNSCR 1718 and its successor resolutions and in UNSCR 1737 and its successor resolutions. However, at the end of the onsite visit, individuals and entities pursuant to the 1737 regime were listed in Türkiye within the scope of UNSCR 2231 which no longer provides for the implementation of TFS since the triggering of the snapback mechanism on 27 September 2025. Over the reporting period, no assets were identified as being held by designated individuals or entities, as well as those acting on their behalf or at their direction which is not fully consistent with Türkiye's identified PF risk and context.

In general, reporting entities' level of understanding and compliance with PF TFS obligations is more limited than for TF TFS, with a severe lack of understanding of PF risks in the DNFBP sector. Competent authorities are undertaking activities to support reporting entities understanding and compliance with PF TFS obligations, but further efforts are needed in this regard.

The approach of monitoring and ensuring PF TFS compliance mirrors the approach for TF TFS and follows a risk-based approach updated yearly. Yet, over the reporting period there were no PF TFS dedicated supervision activities and only a limited number of reporting entities have been supervised for compliance with generic TFS compliance. This coupled with the fact that no violations specific to PF related TFS have been detected in the supervisions conducted so far raises concerns on the effectiveness of supervisory actions on PF TFS compliance. The launch in 2025 of dedicated PF TFS supervision programme is positive but is yet to demonstrate effectiveness.

Türkiye is rated as having a Moderate level of effectiveness for IO.11.

Immediate Outcome 11

618. At the end of the on-site visit (28 November 2025), relevant UNSCRs in force relating to PF were i) UNSCR 1718 (2006) on the Democratic People's Republic of Korea (DPRK) and its successor resolutions 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) and 2356 (2017) and ii) UNSCR 1737 (2006) in Iran and its successor resolutions, 1747 (2007), 1803 (2008) and 1929 (2010).

11.1. Competent authorities' co-operation and co-ordination to combat PF financing

11.1.1. Co-operation and co-ordination to develop and implement policy

619. Türkiye has several co-ordination bodies in relation to combatting proliferation and its financing. Those mechanisms demonstrated effectiveness in setting up several recent policy objectives and documents. The main one is regular interagency co-ordination meetings held under the co-ordination of the Ministry of Foreign Affairs (MFA). These meetings in the larger format bringing together around 20

government agencies and relevant authorities are organized regularly at least twice a year, while meetings in smaller formats are organized more frequently throughout the year, even at short notice, with the aim of assessing non-proliferation related issues as well as export controls, enabling regular meetings with various formats. Türkiye also has the NTFPF for the interagency co-ordination meetings is broader than the scope of PF as per the FATF definition. Under the leadership of the MFA, frequent interagency co-ordination meetings in the areas of disarmament, arms control and non-proliferation and export controls are taking place.

620. Following the adoption of its PF Law (7262) in December 2020 and Regulation on PF (RoPF) in March 2021, Türkiye also established the Commission of Supervision and Co-operation on PF (referred to as the "PF Commission"). Under the leadership of MASAK, the PF Commission gathers representatives from 12 government agencies, most of whom are also members of the NTFPF in addition to three supervisors (BRSA, CMB and Treasury). The PF Commission's mandate is centred on monitoring the implementation of PF related TFS in Türkiye. In addition, a CPF Working Group, under the supervision of the PF Commission, has been established at experts' level in 2025 to specifically assess PF threats and vulnerabilities and support PF risk assessment work.

621. Türkiye has demonstrated effective co-operation and co-ordination to design policies to CFWMD. Their effective implementation could not be assessed by the AT at the time of the onsite visit due to their recent establishment. The PF Commission developed the national PF Strategy Document (2025 - 2029) and Türkiye's first PF NRA (2025) and both documents were published in 2025. The PF Strategy focuses on both the financing of proliferation of WMD and PF risk mitigation, centred around four main objectives namely i) strengthening national co-ordination; ii) enhancing international co-operation; iii) developing supervision mechanisms and iv) ensuring an up-to-date PF NRA. In addition to the PF Strategy, under the lead of MoFA an operational "In-Service Guide on Combating the Financing of the Proliferation of Weapons of Mass Destruction" was prepared in September and disseminated to the relevant ministries and Turkish missions abroad.

11.1.2. Co-operation and, where appropriate, co-ordination for operational purposes

622. Overall, Türkiye's competent authorities demonstrate good co-operation and co-ordination for operational purposes in CFWMD . There is a complementary relationship between the NTFPF and the PF Commission. While the NTFPF primarily focuses on counter-proliferation and export controls, several of its members including MFA, MoT, Intelligence Organisation, Nuclear Regulatory Authority are also members of the PF Commission which focuses on PF related TFS. Hence, authorities involved in monitoring PF TFS are well aware of broader proliferation and financing of proliferation of WMD typologies.

623. Türkiye has established a comprehensive export, import and transit control strategy and framework on dual-use goods and technologies, supported by the operational co-ordination of the various government institutions. The MoT is the authority in charge of monitoring potential unauthorised transfer of dual-use goods and uses different methods (intelligence, profile targeting, inspections) as well as an automated pre-warning system to detect such goods. The PF Commission established lists of dual-use products and "sensitive goods", with a clear list of criteria, for stricter monitoring to be applied for the export or transit of such goods. If there is a suspicion an assessment is made based on the documents showing the technical characteristics of the item and the documents showing the buyer. Opinions from other competent authorities, including foreign counterparts, are frequently asked for according to the nature of the goods. A similar process applies to goods in transit.

624. For DPRK, by law, the sale of any dual-use goods is prohibited and there were no trade relations with DPRK over the reporting period.

625. Türkiye's exports to Iran accounted for approximately 1.2% of the country's total exports and 10% of Iran's total imports in the 2021-2023 period. Iran became Türkiye's 21st largest export partner However, authorities consider that the share of electronics, machinery, chemical and metal products, is close to 40% of which 7% are considered to be sensitive in exports to Iran, including dual-use goods. Since 2019, a total of 33 export authorisation applications for export permits of potential dual-use or sensitive goods exported to Iran or transiting via Türkiye to Iran have been made, including transit of nuclear products. The export of nuclear and dual-use items are subject to prior authorisation from the Nuclear Regulatory Authority, which has not issued any nuclear export permits to Iran since 2019. The MoT authorised 16 of these export authorisation applications, while the remaining 17 were rejected. The authorisations were delivered for goods which would not fall within the dual use category and when needed, where reassurance was provided by the exporting country/institution. Türkiye's Nuclear Regulatory Authority is always consulted before allowing transit authorisation of nuclear products.

Box 11.1. Trade and export controls case studies

Case study 1: Based on information received from relevant institutions, a cargo containing 423 "electronic parts" originating from Country A was to be sent from Country B to Iran through Türkiye. The cargo was halted upon the request of the Ministry of Foreign Affairs. The goods were detected to be listed as part of international PF lists and their transfer to Iran was subject to the authorisation of UNSC including for transit passages. In addition, the country of origin (Country A) did not permit the sale and shipping of the goods. Based on the intelligence that the content of the cargo may be used for Iran's ballistic missile program, the shipping was ceased pursuant to the obligations required under relevant UNSCR and the goods were returned to the sending country (Country B).

Case study 2: Turbojet engines were to be sent from Country C to Iran with transit passage in Türkiye. No information was found to verify the shipping neither by Iranian nor Country C authorities. Further examination did not allow to conclude that purchasing company existed in the name provided nor that it was active. On that basis, the transit shipping was not allowed.

Case study 3: Dual-use goods of other country of origin were planned to be transited via Türkiye to a third country (country D), known as having trade relationship with DPRK. Suspicions emerged due to the specificities of the materials to be transited via Türkiye. As a result of co-operation between competent authorities and information gathering it was concluded that the end user in country E presented a risk of resending the materials to DPRK and the shipment was not allowed. Competent authorities in countries D and E were also informed of the reasons for not allowing the shipment.

11.2. Understanding and mitigating the risk of breach, non-implementation or evasion of PF-related targeted financial sanctions

11.2.1. PF risk understanding

626. The understanding and update of PF risks has been set as a policy objective in Türkiye with the adoption of the PF Strategy Document (2025-2029). As a result, Türkiye completed its first PF NRA in 2025 and is to conduct annual PF risk analyses while fully updating its PF NRA at least once every three years.

627. Competent authorities overall demonstrated a sound understanding of PF risks and this has been enhanced by the work conducting in the development of the first PF NRA. This work was conducted by the PF Commission gathering all relevant competent authorities (see above) and professional associations representing the private sector. Similar to the methodology employed for the ML/TF NRA (see IO.1), Türkiye developed a comprehensive and data-driven PF NRA. It considers the risks of the financing of proliferation of mass destruction as well as both the risks to the effective implementation of sanctions regimes against DPRK and Iran and the risks arising from activities aimed at circumventing these sanctions.

628. Overall, the assessment was based on 76 risk indicators, assessing PF threats—considering both likelihood and impact—and associated vulnerabilities. Among those factors potentially posing PF threats are crimes closely linked to proliferation, as well as economic, commercial, social, and criminal activities of nationals from DPRK and Iran in Türkiye. Trade relationship with these countries and their main commercial partners was also assessed. Additionally, the effectiveness of existing mitigation measures was taken into account in light of the institutional capacities of relevant authorities. The NRA was also prepared with the co-operation of the private sector to a certain extent via the issuance of surveys on TFS compliance (both TF and PF) to sectoral associations to the exception of VASPs, newly regulated sector. The PF NRA also includes a sectoral risk assessment for every FIs, VASPs and DNFBPs establishing the risk exposure of each sector to PF risks.

629. As a result of the PF NRA, Türkiye concluded that its PF risk is relatively low (medium-low), with a medium risk exposure to Iran and a low-risk exposure to DPRK. The overall risk level identified in relation to Iran took into consideration the numerous threats Türkiye is exposed to. Those include Türkiye' strategic position as a regional trade and transit hub, its land border with Iran and the presence of a large Iranian population in Türkiye with a significant portion involved in informal economy and Iranians having partnerships in many companies from different sectors, its trading relationship with Iran including the export and transit of sensitive and dual-use goods.

630. Türkiye demonstrated an overall understanding of evasion of PF related TFS obligation, especially via third country and/or through the use of virtual assets. The PF NRA has a dedicated section on Türkiye's trade of sensitive and dual-use goods with DPRK and Iran main partners and competent authorities have detected typologies of potential sanctions circumvention via jurisdictions that could act as proxy for DPRK and Iran. Beyond the scope of the NRA, and despite the termination of the mandate of the 1718 Committee Panel of Experts in 2024, authorities demonstrated awareness in relation to recent typologies of sanctions evasion by DPRK in collecting information via other international and regional sources. Authorities also considered the increase of virtual asset transactions in global PF typologies as an inherent risk of PF for the circumvention of UNSC sanctions, particularly where this activity involves actors linked to DPRK and Iran.

631. Nevertheless, the NRA analysis on circumvention of PF related TFS is generic and mostly relies on international typologies. Risks related to potential sanction evasions via the misuse of legal persons are understood to a lesser extent and could hinder Türkiye's ability to deter PF risks to some extent. Challenges in obtaining accurate and up-to-date BO information (see IO.5), reinforces risks related to the misuse of front and shell companies to impede PF detection efforts.

11.2.2. PF risk mitigation

632. The PF Strategy Document and the PF NRA support the implementation of mitigating measures to some extent, but actions are still to be taken in light of their recent adoption. As part of the NRA, strategic analysis studies were conducted using data such as STRs, foreign currency transfers, company asset size, import and export data, foreign sales, central province, date of establishment, and number of employees, with the aim of preventing the potential circumvention of sanctions against Iran, preventing the misuse of the Turkish financial sector, and preventing illegal money flows. As a result of the analysis, the activities of a total of 139 companies were found to be suspicious, and a more comprehensive operational analysis study was initiated. The operational analysis of 65 of these companies was ongoing at the time of the onsite visit. The data obtained as a result of this analysis is planned to be shared with the relevant competent authorities. MASAK also issued in October 2025 a PF guideline for reporting entities.

633. In Türkiye, reporting entities can send STRs specifically on PF since May 2024. STRs received by MASAK after this date are not directly related to PF, and reporting entities have so far resorted to defensive reporting on their customers related to high-risk jurisdictions, further outreach to enhance the awareness of reporting entities on PF is needed (see 11.5).

634. As a result of STRs analysis, MASAK also disseminated strategic analysis for operational purposes to competent authorities to mitigate PF risks. Over the reporting period, MASAK received 167 STRs related to PF, and approximately 1 000 STRs were submitted to MASAK in relation to Iran nationals and 180 in relation to DPRK. None was linked to potential PF activity, but other predicate offences such as fraud, illegal betting and drugs trafficking. The absence of PF related STRs is not in line with Türkiye's risk exposure.

635. Operational analysis is also conducted in relation to DPRK and Iran, yet there is no clear finding of PF related activities. In 2025, a detailed operational analysis was conducted on 46 individuals and legal entities allegedly associated with Iran. Findings were shared with LEAs and intelligence units and supervisory authorities. An information note regarding 16 legal persons and 1 natural person assessed as potentially linked to DPRK was shared with the National Intelligence Organization and the MoT. Additional research was also conducted regarding potential cryptocurrency transfer transactions claimed to be related to DPRK involving the individual mentioned in STR. No data was found indicating that the legal person subject to the analysis has direct links to DPRK and it was assessed that the matter was not related to DPRK. In 9 cases where suspicious transaction reports were filled in relation to DPRK, transactions were rejected.

636. Some reporting entities, especially large banks, apply mitigating measures in relation to PF due to their international exposure via correspondent banking relationships, taking into consideration domestic, UN and foreign based sanctions lists. In foreign trade payments intermediated by banks, especially within the scope of intermediation of trade payments for high-risk countries, some entities have controls over documents such as customs declaration, bill of lading, certificate of origin, etc. Within this framework enhanced due diligence measures are applied in relation to customer and BO identification. Those entities also resort to commercial databases and software to search for a possible match on a sanction list regarding one of the customers and vessels involved in the shipment.

11.3. Implementation of PF-related targeted financial sanctions without delay

637. Türkiye has a similar mechanism for the implementation of PF and TF TFS which ensures implementation without delay to some extent but does not ensure application without delay in a consistent manner (see IO.10). TFS pursuant to UNSCR 1718 and its successor resolutions and pursuant to UNSCR 1737 and its successor resolutions are not immediately enforceable in Türkiye upon UN designation. While the process has allowed for the implementation of TFS without delay, it takes on average two and a half days for TFS to be enforceable in Türkiye. The time required for the UN listing decision to be transposed

into domestic law impedes Türkiye's ability to implement TFS without delay. The mechanism described under IO.10 to address to some extent delay in domestic transposition does not apply for PF TFS (see Rec 7).

638. Türkiye has been applying PF related TFS on DPRK and Iran since 2021 and has listed individuals and entities accordingly, in line with relevant UNSCRs and the FATF Standards for the vast majority of the reporting period. As of the end of the onsite visit, Türkiye has listed individuals and entities included in UNSCR 1718 and its successor resolutions and in UNSCR 1737 and its successor resolutions. However, at the end of the onsite visit, individuals and entities pursuant to the 1737 were listed in Türkiye within the scope of UNSCR 2231 which no longer provides for the implementation of TFS since the triggering of the snapback mechanism on 27 September 2025[43].

639. As described under Recommendation 7, Türkiye's legal framework for the implementation of PF TFS is composed of a Law, Regulation and Presidential Decrees. The PF Law (7262) provides for a legal basis on the application of TFS on UNSC resolutions "on the sanctions for countering the financing of the proliferation of mass destruction weapons" without a reference to specific UNSCRs to be able to include all relevant UNSCRs. The principles and procedures of the PF Law are further defined in a Regulation (RoPF) and the implementation of PF related TFS through the adoption of Presidential Decrees.

640. The RoPF identifies UNSCR 1718 (2006) and successive resolutions and UNSCR 2231 (2015) and successive resolutions as the two regimes for the implementation of PF related TFS. In line with the RoPF, Türkiye has adopted and gazetted ten Presidential Decrees since 2021 for the implementation of PF related TFS. Among those, three Presidential Decrees- respectively adopted in February 2021, August 2022 and October 2025 – are adding individuals and entities on the domestic list, while the seven remaining Presidential Decrees updated the information of persons and entities on the list. Those Presidential Decrees explicitly mention that they are implementing PF related TFS in the scope of UNSCR 1718 and successor resolutions and of UNSCR 2231.

641. For PF related TFS on Iran, UNSCR 2231 does no longer provide for the implementation of TFS since the triggering of the snapback mechanism of UNSCR 2231. At the end of the onsite visit, Türkiye had not amended the RoPF nor the Presidential Decrees to implement TFS on the basis of UNSCR 1737 and successor resolutions. While Türkiye had been implementing PF related TFS since 2021 and during a large part of the reporting period, at the end of the onsite visit, despite the listing of individuals and entities, it could not be considered that Türkiye was implementing PF related TFS on Iran in line with the relevant UNSCRs nor with the FATF Standards since 27 September 2025.

11.4. Identification of assets and funds held by designated persons/entities/those acting on their behalf and prohibitions

642. Over the reporting period, no assets were identified as being held by designated individuals or entities, as well as those acting on their behalf or at their direction. There was one case of false positive identified in 2024 (see below). The absence of PF-related funds or assets related to DPRK and identified by Türkiye, is compensated to some extent by mitigating measures and investigations into potential cases. Yet there are residual concerns regarding whether the lack of identification is reasonable given Türkiye's

[43] In line with the process set forward in paragraphs 11 and 12 of UNSCR 2231 (the Snapback Mechanism), all provisions of UNSCRs 1696, 1737, 1747, 1803, 1835 and 1929 that have been terminated pursuant to paragraph 7 of UNSCR 2231 shall apply in the same manner as they applied before the adoption of UNSCR 2231 on 20 July 2015. Four of these six UNSCRs - 1737, 1747, 1803 and 1929 (collectively referred to as the Iran TFS UNSCRs) - identify targeted financial sanctions that, in accordance with FATF Recommendation 7, must be applied. The obligation to implement those targeted financial sanctions was effective immediately for all UN Member States on 27 September at 8:00 p.m. Eastern Daylight Time. See FATF/PLEN(2025)71.

exposure, arising from its status as regional financial and trade hub. The absence of identification of PF cases in relation to Iran is not fully consistent with Türkiye's identified PF risks and context.

643. As described below, reporting entities understanding of PF TFS is limited and in the best cases is focusing on the requirement to detect positive matches against sanctioned individuals and entities through screening. The lack of understanding and consideration of more complex sanctions evasion techniques, coupled with the reliance on commercial databases to identify listed natural and legal persons, do not support potential identification of more complex TF schemes including of persons acting on behalf or at the direction of UN designated persons and entities. In addition, as highlighted in IO.3 and IO.4, smaller FIs and DNFBs face challenges in identifying and/or verifying BO, particularly involving complex structures or foreign ownership. This weakens Türkiye's ability to detect and prevent sanctions evasion schemes, particularly those involving individuals acting on behalf of or exerting indirect control over designated persons or entities.

Box 11.2. False positive case study

In January 2024, MASAK was informed of a potential match during an attempted transaction in the land registry. Initial inquiries revealed that a person named Mr A, known to have served as a Rear Admiral in the Iranian Revolutionary Guard Corps, had been designated under UNSCR 2231 and had his assets in Türkiye frozen by a Presidential Decision. Upon a detailed inquiry by MASAK and verification of the identity information, it was determined that the individual was not the same person as the one designated under the UNSC sanctions list. Land registry was informed of the false positive case.

11.5. FIs, VASPs and DNFBPs understanding of and compliance with obligations

11.5.1. FIs and VASPs

644. In general, reporting entities' level of understanding and compliance with PF TFS obligations is more limited than for TF TFS.

645. Banks have a better understanding of their PF TFS obligations and of PF risks in general than other reporting entities. They are overall aware of potential cases of breach or non-implementation of TFS, as well as of more sophisticated ways of evading PF, identifying jurisdictions, beyond DPRK and Iran, that can be used for sanctions evasion, typologies related to the financing of dual use goods and transhipment risks. Banks in Türkiye clearly identify risks emanating from Iran as their main PF exposure. Banks understanding of their PF risks has been supported by two specific PF surveys circulated to the sector by the Banks Association of Türkiye and BRSA. The fact that the banking sector in Türkiye is highly connected to the international financial system with Turkish banks having branches abroad and being sensitive to UN as well as other domestic sanction regimes has enhanced sectoral efforts to understand and comply with PF requirements. However, in light of Türkiye's context, the over reliance on commercial screening software may not support the identification of those acting on behalf or at the direction of UN designated persons and entities.

646. VASPs' understanding of PF related TFS is limited to screening requirements rather than obligations related to the detection of those acting on behalf, or at the direction of, designated persons and entities. As for TF TFS, banks and VASPs comply with their PF TFS to a large extent, relying on international monitoring programs and software and applying daily screening to their customer database and/or transactions.

647. Other FIs are aware of their obligations to comply with UN lists screening however they have a vague to negligible understanding of the PF risks they are exposed to. Some entities are not aware of the difference between TF and PF TFS and a few representatives the assessment team met with considered that there was no PF risk in their sector. Those entities comply with their PF TFS obligations in a similar way as to their TF TFS ones. As highlighted under IO.10, except for banks and VASPs, most other FIs rely on manual screening, the lack of systematic updates and understanding of the specificities of PF TFS requirements can cause delays or even lack of PF TFS compliance.

11.5.2. DNFBPs

648. There is a severe lack of understanding of PF risks in the DNFBP sector and some have a limited understanding of the concept of beneficial owner (see IO.4), which impede the sector ability to identify methods of evading PF TFS beyond list screening. DPMS and REAs have some knowledge of their obligations related to UN lists screening but those are only performed at the onboarding stage and there is no awareness within those sectors that they can be used to evade sanctions regimes, including by those acting on behalf of designated persons and entities. Accountants and legal professions did not demonstrate awareness of their PF TFS obligations, including lawyers whose clients are international transhipment companies. Given Türkiye's exposure to PF risks, especially from one of its neighbouring jurisdictions, DNFBP's lack of understanding of PF risks and related obligations is a concern.

649. Competent authorities' efforts to support reporting entities understanding and compliance with PF TFS obligations is effective to a limited extent. At the time of the onsite visit, most actions were still to be developed or just recently adopted. A generic guidance on TFS obligations for reporting entities was published in 2022 without specific details for the specificities of PF related TFS. Authorities also adopted and made public in 2025 both Türkiye's PF Strategy Document (2025-2029) and a PF NRA (2025) and outreach activities to raise awareness on those findings are ongoing. Türkiye also amended its legal framework end of 2024 to request that reporting entities' institutional policies include the monitoring and mitigation of the risks of violation, non-implementation and avoidance of asset freezing decisions as well as enhanced controls for the implementation of both TF and PF TFS. This measure is still being implemented.

11.6. Competent authorities monitoring and ensuring compliance with PF-related targeted financial sanctions

650. The approach for monitoring and ensuring PF TFS compliance mirrors the approach for TF TFS (see IO.10). In line with its 2021 ICRG Action Plan, Türkiye implemented a risk-based approach for monitoring reporting entities compliance with TFS obligations, by developing separate supervision programmes based on a separate risk analysis specifically for TFS monitoring, both in terms of TF and PF. On an annual basis, competent authorities assess reporting entities risk level for TFS compliance taking into consideration several factors such as control measures applied by reporting entities, asset size, outcome of previous inspections. Within each sector, reporting entities are then categorised into high/medium and low TFS risk and authorities conduct onsite inspections to all high risks entities and some medium risks. Apart from planned inspections, if evidence emerges that an obligated party has violated the sanctions, that party is supervised independently of the program, and sanctions are imposed in case of violation. Periodic inquiries are also conducted to determine whether individuals and legal entities on asset freeze lists have committed any violations following the freeze decision. Yet, this approach led to the monitoring of an overall limited number of reporting entities over the reporting period, Türkiye could make wider use of offsite supervision to expand the scope of entities supervised on PF related TFS obligations.

651. Violations related to TF TFS were detected in the supervisions of the banking, MVTS and insurance sectors (see IO.10) but not for PF TFS. The PF NRA recognises that the systems of the relevant companies were not sufficiently capable of handling TFS, including related to PF. This coupled with Türkiye unique position as a regional financial and transit hub and its specific risk exposure to Iran, and the specific risks related to potential breaches and evasions of sanctions which is taken into consideration to a limited extent by some reporting entities could likely to result in more PF violation risks.

652. Building upon the results of the PF NRA, authorities decided in 2025 to differentiate the risk analyses for TF related and PF related TFS in order to carry out separate supervisions with better risk understanding and better scoping either on TF or PF. As of the time of the onsite visit, the supervision programmes had not been finalised but the plan was for supervisors to inspect 147 entities, among which 108 FIs and 39 DPMS/REAs, following a risk-based approach. Türkiye's plan to prioritise the supervision of the entities posing the highest risk within the sectors most at risk of PF according to the PF NRA results is a positive development, however the effectiveness of such measure is yet to be demonstrated.

Annex A. Technical compliance[44]

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

This technical compliance annex covers areas where the country has made legal, regulatory or operational framework changes since its last mutual evaluation (dated December 2019) (or follow-up reports with technical compliance re-ratings (dated May 2021, and June 2023) and areas where there has been a change in the FATF Standards for which the country has not previously been assessed. The reassessed areas are clearly identified under each heading.

For Recommendations not under review, pre-existing information from the country's most recent assessments is included. Such Recommendations are marked with a footnote cross-referencing the date and source of the information (i.e. the country's most recent mutual evaluation or follow-up reports with technical compliance re-ratings).

Recommendation 1 – Assessing risks and applying a risk-based approach[45]

In its 2019 MER, Türkiye was rated largely compliant with R.1 primarily because of minor shortcomings regarding dissemination of risk assessment results to all FIs and DNFBPs and lack of requirements for DNFBPs to apply enhanced measures to risks identified. Recommendation 1 was since revised to require assessing and mitigating PF risks.

Countries' obligations and decisions

Assessment of ML/TF risks

Criterion 1.1

Türkiye identifies and assesses ML/TF risks including through its National Risk Assessment (NRA). Türkiye prepared its first NRA in 2018 and updated it in 2023 and 2025. The NRAs include an overview of the most relevant proceeds generating predicate crimes, predominant sectors abused for ML and ML methods, consideration of national and international threats relevant to TF and vulnerabilities associated with the financial (VASPs are considered financial institutions (FIs) in Türkiye) and DNFBP sectors.

Criterion 1.2

Türkiye designated MASAK as the competent authority to co-ordinate actions to assess risks (Presidential Circular 2021/16). PD No.1 authorises MASAK to co-ordinate risk assessment studies on ML/TF at the national level (article 231(1)(a)).

[44] In accordance with the 5th Round Methodology, Recommendations under review, which have been analysed for this mutual evaluation, are in green.

[45] Recommendation 1 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

Criterion 1.3

Türkiye keeps its risk assessments up-to-date as noted under 1.1. Türkiye conducted its first NRA in 2018, with updates in 2023 and 2025.

Criterion 1.4

Türkiye has mechanisms to provide information on the results of the risk assessment(s) to all relevant competent authorities and the private sector. The 2023 and 2025 NRAs conclude with an action plan which MASAK disseminated to the relevant organisations, competent authorities together with the full NRA report itself. A public summary version of the NRAs is available on MASAK's website[46] to ensure further implementation by stakeholders. It also assists that the NRA was the result of a collaborative effort by different competent authorities and the private sector. Thus, public agencies involved in Threat and Vulnerability Working Groups and private sector representatives such as professional unions and associations (SRBs) contributing to the NRA preparation phases acquired and continue to acquire knowledge from the beginning of the process.

MASAK also provided and continues to provide information to the private sector through workshops. Türkiye organised 31 workshops for FIs/VASPs and 31 workshops for DNFBPs during the period under review. MASAK prepared and delivered ML/TF Typology Reports in 2024 to regulatory and supervisory bodies and private sector representatives (Strategy Document Target 1.3, activity 1.3.g; NRA Action Plan, Target 1, Item 1.1) and has done the same for 2025 according to the 2025 NRA and action plan.

Assessment of PF risks

Criterion 1.5

a) Türkiye prepared its first PF NRA in 2025. A unique methodology was developed in Türkiye to measure PF risks, based on PF threats and vulnerabilities (emanating from PF factors, likelihood and impact). Moreover, impact of mitigating measures was also estimated for considering net risk, based on the capabilities of relevant authorities. A summary version of the report has been uploaded to MASAK's website[47].

d) Türkiye designated the Commission on Supervision and Co-operation (PF Law, art. 4) for the implementation of the PF law, as well as the supervision of implementation and any form of co-operation related to PF. MASAK is assigned to carry out secretariat work, which includes collecting and discussing information for assessing risk though not explicitly mentioned as demonstrated by the PF NRA. The Commission on Supervision and Co-operation took the decision to prepare a PF NRA in Türkiye in its meeting on 3 November 2023 and a PF Working Group was formed under the co-ordination of MASAK. Officials from the agencies represented in the Commission on Supervision and Co-operation participated in the working group activities. Data and information from other relevant stakeholders were sought during the risk analysis process. The PF NRA was adopted by the Commission on 28 February 2025.

e) Türkiye is required to prepare a PF NRA and keep it up-to-date in accordance with the risks identified (PF Strategy, Strategic Objective IV), which includes aiming to analyse PF risks annually and to update the PF NRA in three years at the latest.

f) Türkiye has mechanisms to provide information on the results of the PF NRA to all relevant competent authorities and SRBs, FI, VASP and DNFBPs. Besides uploading a version of the report to the MASAK website, a summary of the PF NRA was sent electronically to a large portion of FIs as well as the associations and unions of DNFBPs so as to be disseminated to all obliged entities and used in workshops to be conducted in line with the PF NRA Action Plan.

[46] https://ms.hmb.gov.tr/uploads/sites/2/2025/06/2023-NRA-Summary-c6e72d9fc81e3757.pdf .

[47] https://ms.hmb.gov.tr/uploads/sites/2/2025/09/NRA-2025-Summary-02bd6dfcdb75f9ce.pdf.

Measures to mitigate ML/TF risks

Criterion 1.6

Based on its understanding of its risks, Türkiye applies a risk-based approach to allocating resources and implementing measures to prevent or mitigate ML/TF including as demonstrated in IO.3. NRA action plan target 3 is about improving the supervision capacity and level of compliance by the obliged parties. Activity 3.4 in the NRA 2023 and Activity 3.3 in the 2025 NRA are about incorporation of the NRA results in the compliance programs of relevant FIs/VASPs/DNFBPs.

Criterion 1.7

Türkiye has not decided "not to apply" some of the FATF Recommendations. Türkiye has not applied any exemptions.

Criterion 1.8

Türkiye ensures the AML/CFT regime addresses higher risks where these are identified, by requiring enhanced due diligence measures (EDD) for specific transactions and high-risk situations identified by FIs and DNFBPs (RoM, art. 18, 20, 25). There are specific requirements for FIs and DNFBPs to take risks that have been considered as high by authorities into account in their risk assessments and to implement EDD measures. EDD measures include obtaining additional information on the customer and updating more regularly identification data of the customer and BO; obtaining information on the intended nature of business relationship, information on the source of the assets subject to transaction and source of the funds of the customer; among others (RoM, art. 26/A).

Criterion 1.9

Türkiye allows FIs and DNFBPs to take simplified due diligence (SDD) measures in specific circumstances assessed as low risk and in such other low risk circumstances as the Ministry of Treasury and Finance may decide (RoM, art. 26). In addition, simplified measures may not be applied where ML/TF risks are identified. MASAK Communiqué No. 5 provides further clarity on cases where simplified measures can be applied.

Criterion 1.10

Supervisors and SRBs ensure that FIs and DNFBPs are implementing their obligations under R.1 through risk-based supervision as explained under c.1.6 above and R.26 and R.28.

Measures to mitigate PF risks

Criterion 1.11

Based on its understanding of risk, Türkiye implements risk-based measures, commensurate with the risks identified and allocates resources efficiently, to mitigate PF risks, and

a) Türkiye has not explicitly applied any exemptions from requirements to identify, assess, monitor, manage or mitigate PF risks.
b) Where Türkiye identifies higher risks, it requires FIs and DNFBPs including based on their risk assessment to implement measures commensurate to those risks (RoC, art.7). The legislative framework in Türkiye on countering proliferation financing, financing of terrorism and money laundering complement each other. The PF Law refers to the TF Law and the TF Law refers to the AML/CFT Law No. 5549 to prevent any legislative gaps (PF Law, art 3[4]. Legislation adopted in line with the Law No. 5549 and 6415 are applicable unless a different direct provision exists to the contrary.
c) Where Türkiye identifies lower risks, for FIs, it ensures measures applied are commensurate with the level of PF risks, while still ensuring full implementation of R.7 (RoC, art.7 and explanation above

on how the TF law applies to PF). In cases where the risk of ML/TF are assessed as low in terms of transaction types, SDD measures are applied. This provision is applicable for PF as well. Moreover, within the PF NRA, the vulnerable sectors, regions and products are discussed and FIs and DNFBPs are ranked in terms of their ML/TF risks and during the updates of MASAK General Communique No. 5, PF NRA results are also taken into account as it is mentioned in c.1.9 above, and as stipulated in MASAK General Communique 5, where Türkiye identifies lower risks, it ensures measures applied are commensurate with the level of PF risks, while still ensuring full implementation of R.7 (RoM art. 26, RoC, art. 7).

d) MASAK as the AML/CFT supervisor ensures FIs and DNFBPs are implementing their obligations regarding PF risk under R.1 (PF Regulation, art.17).

Obligations of financial institutions and designated non-financial businesses and professions

Assessment of ML/TF risks

Criterion 1.12

FIs and DNFBPs (considering business size, business volume and the nature of the transactions they conduct; RoC art. 32A, art. 14 and 15) are required to take appropriate steps to identify, assess, and understand their ML/TF risks (for customers, countries or geographic areas; products, services, transactions and delivery channels). This includes being required to:

a) Document their risk assessments. Policies and procedures must be in written form (RoC, art. 9(1)). This article, combined with arts. 7, 11 and 12, mean risk assessments (which are required) must be in written form.

b) Consider all relevant risk factors before determining what is the level of overall risk and appropriate level and type of mitigation to be applied including customer, service and country risk (RoC art. 12). In addition to the factors mentioned above in this criterion, other relevant risk factors include: risky countries (RoM, art. 3(1)(i)); transactions requiring special attention (RoM, art. 18); monitoring the customer profile and transactions (RoM, art. 19); taking measures against technological risks, which includes risks of new and existing products and delivery channels (RoM, art. 20); rejection of transactions and termination of business relationships (RoM, art.22); relationships with risky countries (RoM, art. 25); and enhanced measures (RoM, art. 26/A), as well as: service risk (RoC, art. 3(1)(c)); customer risk (RoC, art. 3(1)(d); risk of financial loss or reputational damage (RoC, art 3(1)(f); country risk (RoC, art. 3(1)(i); additional measures for high-risk groups (RoC, art. 13) and monitoring and controlling (RoC, arts. 14 and 15).

c) Keep assessments up to date, as Türkiye requires compliance programme and risks management activities be reviewed and updated every two years or as necessary based on risk perception (RoC, art. 5).

d) Have appropriate mechanisms to provide risks assessment information to competent authorities and SRBs as Türkiye requires FIs and DNFBPs to send their institutional policies to MASAK (RoC, art. 9). These policies cover risk assessments.

Measures to mitigate ML/TF risks

Criterion 1.13

a) FIs and DNFBPs are required to have policies at a minimum relating to risk management, monitoring and controlling, training and internal audit and entities part of financial groups are required to have policies regarding information sharing within the group (RoC, art. 7). Procedures must be put in place for certain issues, such as who is responsible for measures and operations under the institutional policies created in accordance with RoC art. 7, and which persons/units are

responsible for ratifying, carrying out, reporting and monitoring transactions according to the determined risk (RoC, art. 8). Policies and procedures must be ratified by the Executive Board(RoC, art. 6 (2)). See (sub-criterion b) below for internal controls). The Executive Board is responsible for the review, monitoring and timely adjustment of the compliance programme (RoC, art 6(2)).

b) The contents of compliance programmes (institutional policy and procedures; risk management; monitoring and control activities; assignment of a compliance officer and compliance unit; training; internal control activities) are clearly specified (RoC, art. 5). Monitoring and control requirements for customers are specified (RoC, arts. 14 and 15). Further detail, including that deficiencies must be reported to the Executive Board, are also clearly specified in law (RoC, arts. 26 and 27). Deficiencies detected as a result of monitoring and control measures must be reported to the relevant units for the necessary measures to be taken, and the results must be followed up (RoC, art. 15(1)).

c) Regarding additional measures (to the risk management procedures above, which include dealing with high risk in general) where higher risks are identified, for example, when establishing business relations with VASPs, FIs are required to take additional measures and collect information on the sources of funds subject to the transaction, on the purpose of the transaction and applying increased scrutiny on the business relationship by increasing the number and frequency of the controls (RoC, art 13(2)). In addition, when payment and e-money institutions conduct a transaction requiring a business relationship or CDD they are required to take all enhanced due diligence measures (RoC, art 13(3)).

Criterion 1.14

See c.1.9. SDD measures can only be applied in relation to the types of transaction specified by legislation or by the Ministry of Treasury and Finance and are not permitted if there is a ML/TF suspicion.

Assessment of PF risks and measures to mitigate them

Criterion 1.15

Please see c.1.12 to 1.14 as same provisions apply regarding PF as required explicitly/extended to by art. 7 of the RoC.

Weighting and conclusion – All criteria are met. Recommendation 1 is rated **compliant**.

Recommendation 2 – National co-operation and co-ordination[48]

In its 2019 MER, Türkiye was rated largely compliant with R.2 because it lacked overarching, national strategies and policies to combat ML/TF informed by the risks which were since developed. R.2 was revised since to include further requirements regarding co-operation and co-ordination regarding PF.

Criterion 2.1

Türkiye has the following national AML/CFT/CPF policies which are informed by risks identified, including in its NRAs, and are regularly reviewed (e.g. at least every two years for ML/TF and every three years for PF; AML/CFT Strategy Document, activity 2.2. (c) and the PF Strategy Document, activity 4.1.b.): its "Strategy Document on Increasing Effectiveness in Confiscation, the Fight Against Money Laundering and Financing of Terrorism in Türkiye (2021-2025)" and "Strategy Document on Increasing Effectiveness in Countering the Proliferation of Weapons of Mass Destruction in Türkiye (2025-2029)". These documents are complemented by agency and working group- level strategies, action plans, committees, working groups and similar mechanisms dealing with TF separately and Türkiye's main predicate offences, as well as other

[48] Recommendation 2 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

aspects (e.g. financial inclusion) some of which are described in Türkiye's 2023 and 2025 NRA and form part of Türkiye's fight against ML/TF.

Criterion 2.2

Türkiye has an inter-agency framework in place to enable policy makers, the Financial Intelligence Unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities to co-operate and where appropriate, co-ordinate and exchange information domestically with each other concerning the development and implementation of AML/CFT/CPF policies.

The National Security Council (NSC) is the primary mechanism for preserving Turkish integrity, independence and security (Constitution, art. 118). The NSC's role is broad in scope, and its mandate includes terrorism in all its aspects, including TF. The National Intelligence Co-ordination Board (NICB) acts as a high-level co-ordination mechanism (Law No. 2937, art. 5). MASAK is represented in the Board to cover AML/CFT issues. Among other tasks, MASAK is required to develop policies and implement strategies to ensure co-ordination amongst institutions and organisations for the prevention of ML(PD No. 1, art. 231). The Co-ordination Board for Combating Financial Crimes (CBCFC), chaired and administered by the Deputy Minister of MoTF, is the main tool for AML/CFT co-ordination. In addition to MASAK, which serves as the Secretariat for the CBCFC as its membership comprises a range of government representatives and supervisory authorities (PD No. 1, art. 232, and Regulation 26730), there is also an Internal Security Strategies Co-ordination Board (ISSCB), the members of which are affiliated with the Ministry of the Interior. The functions of the ISSCB and working groups that report to the ISSCB include the formulation of strategies, policies and action plans on national security issues (including terrorism and TF), and the monitoring of their implementation.

On PF, Türkiye has the Commission on Supervision and Co-operation, which comprises the relevant competent authorities such as MASAK, Ministry of Justice, Ministry of Foreign Affairs, Ministry of Energy and Natural Resources, Ministry of Interior, Ministry of Defense, Ministry of Trade, Banking Regulation and Supervision Agency, Treasury Comptrollers Board, National Intelligence Organization, Nuclear Regulation Authority and Capital Market Board (Law 7262, art. 4). If deemed necessary, other competent authorities may also be invited to the said Commission.

Türkiye established a Threat, Vulnerability and Sanctions Working Group (Presidential Circular No. 2021/16) and a PF Working Group (Presidential Circular No. 2025/5). These working groups meet more frequently to discuss relevant matters at the practitioner / expert level. Türkiye also established a Working Group on Combating PF consisting of representatives of the relevant units of the Commission on Supervision and Co-operation (PF Strategic Document, Target 1.2).

Criterion 2.3

MASAK is the responsible authority for setting AML/CFT/CPF national policies and ensuring co-operation and co-ordination (PD 1, art 1(a)). The Commission on Supervision and Co-operation is designated by law as the CPF policy developing and co-ordinating body but MASAK plays a key role as the Secretary to the Commission (Law 7262, art. 4(1)).

Criterion 2.4

See c.2.2 and 2.3 for the policy-making mechanisms in Türkiye. The Co-ordination Board for Combating Financial Crimes (CBCFC), chaired and administered by the Deputy Minister of MoTF, is the main tool for AML/CFT co-ordination. MASAK acts as Secretariat of the CBCFC. Türkiye has a dedicated case working group for following up on qualified ML/TF cases. Other operational-level mechanisms include the Assessment Commission and a Virtual Currency Working Group relevant to the implementation of TFS and discussion of vulnerabilities respectively. Relevant documents include the Action Plan on CFT, the National Strategy on Fighting Organised Crime (which includes an Action Plan), the National Anti-Drug Strategy

Paper and Combatting Drugs Action Plan (which includes ML and narco-terrorism issues). There are also strategy papers and Action Plans that seek to address aspects of predicate criminality, which are relevant to reducing ML.

Türkiye has implemented the following interrelated action plans and strategy documents in the fight against predicate offences, ML and TF:

a) Strategy Document on Combating Laundering Proceeds of Crime and Financing of Terrorism and Increasing Efficiency in Confiscation Practices in Türkiye (2021-2025): The document aims to improve the country's capacity to combat ML/TF through 44 activities under 5 strategic objectives and 15 targets to combat ML and TF. The Strategic Objectives identified within the scope of the document are listed below:
    i. Effective execution of judicial and administrative processes related to ML/TF,
    ii. Ensure that the national risk assessment for combating ML/TF is up to date.
    iii. Prioritisation of judicial and administrative processes involving financial aspects of ML/TF in line with national risk assessment results.
    iv. Assess the legislative infrastructure and effectively implement all judicial and administrative measures to seize and confiscate assets derived from crime in the context of the ML/TF and related predicate offences.
    v. Carrying out studies to ensure the effective use of targeted financial sanctions within the scope of combating TF.
b) The "2022-2027 National Strategy Document on Combating Organised Crime" and "2022-2024 Action Plan on Combating Organised Crime": These documents are designed to minimise the impact of organised crime, which requires a multifaceted and effective fight. The document was designed in co-ordination with the AML/CFT Strategy Document (2021-2025) in order to improve the systematic fight against money laundering and terrorist financing.
c) Strategy Document on Combating the Financing of Terrorism is an umbrella document that aims to define the priorities of Türkiye's fight against terrorism and combating the financing of terrorism in a co-ordinated manner and aims to improve co-operation and co-ordination among relevant institutions, improve legislative capacity and increase the impact of operational activities. The document entered into force with the Presidential Circular No. 2022/13.
d) National Strategy Document and Action Plan for Combating Drugs (2024-2028): The "2024-2028 National Action Plan and Strategy Document on Combating Drugs" entered into force with the aim of determining the road map of our country in the fight against drugs, including consumption prevention.
e) Action Plan for Combating Fuel Smuggling (2021-2023). Included establishing a task force/joint work as described in IO.7.
f) Action Plan for Combating Informal Economy (2023-2025): The Action Plan includes 44 actions under 5 main components. These components are as follows: a) Measurement and Analysis of the Size of the Informal Economy (3 Actions); b) Raising Social Awareness and Voluntary Compliance (6 Actions); c) Improving Inter-Agency Co-operation and Data Sharing (4 Actions); d) Taking Legal, Administrative and Technical Measures (25 Actions), and e) Enhancing Audit Capacity (6 Actions).
g) National Strategy Document and Action Plan for Combating Behavioural Addictions (2024-2028): Within the scope of the document, a plan consisting of 1 final objective, 3 intermediate objectives, 13 initiatives and 75 activities was prepared to take preventive, treatment and rehabilitative measures against excessive and harmful technological content and gambling addiction.
h) Within the scope of the activities of the High Council for Combating Addiction, which is chaired by the Vice President and co-ordinated by the Minister of Health, MASAK has also been assigned responsibilities in the fight against illegal betting on online sites.

i) Strategy Document and National Action Plan for Combating Irregular Migration (2021-2025):Within the scope of the document, strategic priorities were identified for preventing irregular migration at source, increasing border security, managing foreign labour migration, protecting irregular migrants with a focus on human rights, ensuring their integration and repatriation, and it was aimed to implement these priorities in line with the contributions of all public institutions and organizations and non-governmental organisations.

j) Siberay (Cyber-Moon) Project (2020-): It is a project that aims to raise awareness of citizens of all age groups in order to ensure safe and conscious internet use and to create cyber awareness in the field of cyber security, with the opening meeting held in Ankara on September 29-30, 2020. Within the scope of the Siberay Project, which has sub-components of Cyber World, Cyber Security, Digital Gaming and Combating Digital Addiction, it is a project that aims to increase the level of awareness of the public against cyber-attacks and addiction.

k) Strategy for Increasing Effectiveness in Combating Illegal Betting in Türkiye (2023-2027): Taking inspiration from the success of the Siberay Project, work is underway under the co-ordination of the TNP Department of Combating Cybercrimes to prepare a country strategy for the establishment of a working group with the participation of all relevant institutions in the field of combating illegal betting and a High Council for Combating Illegal Betting in the field of policy making.

l) Action Plan for Combating Fraud: Drafting of the aforementioned action plan is ongoing. The draft action plan was opened to the opinions of relevant public institutions and organisations and included analysis and deliberations and ongoing discussion which were relevant to this criterion even where the final plan is not implemented.

Criterion 2.5

MASAK, along with other law enforcement authorities, co-operates and co-ordinates with the Turkish Personal Data Protection Authority, established under Law No. 6698. This includes participation in drafting of legislation (ensuring compatibility of AML/CFT/CPF requirements as matters of for example, national security, are outside of the scope of Law No. 6698 (data protection) and in training programmes on data protection and privacy issues.

Weighting and conclusion – All criteria are met. Recommendation 2 is rated **compliant.**

Recommendation 3 – Money Laundering offence [49]

In its 2019 MER, Türkiye was rated largely compliant with R.3. The main technical deficiencies remaining were that the legislation covered the concealing or disguising assets only when conducted with a specific intention and self-laundering applies to the act of purchasing, possessing, etc., with the intention of disguising or concealing the illicit source of funds and that ML offences sanctions for legal persons (administrative fines) are not dissuasive.

Criterion 3.1

The ML offence covered in the TCL is broadly in line with the Vienna and Palermo Conventions as material elements are covered as follows:

a) Conducting any act, for the purpose of concealing or disguising the illicit origin (TCL, art. 282(1)) which covers the conversion or transfer of assets, as required by the conventions. However, concealing, or disguising assets are only covered when they are conducted with a specific intention.

[49] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from Türkiye's 2019 MER except for very minor edits by Türkiye.

b) Purchase, acquisition, possession or use of illicit funds constitute an ML offence for third-party launderers (TCL, art. 282(2)) and self-launderers under the specific intention of concealing or disguising illicit proceeds (TCL, art. 282(1)).

Criterion 3.2

Predicate offences to ML constitute all offences that carry a minimum penalty of six months' imprisonment (TCL, art. 282(1)). This covers a range of offences in each FATF designated categories of predicate offences.

Criterion 3.3

Türkiye applies a minimum threshold approach, where the predicate offence carries a minimum penalty of six months' imprisonment.

Criterion 3.4

The ML offence extends to any asset, which has been acquired as a result of an offence (TCL, art. 282(1)). The term assets refer to money, any kind of movable or immovable, tangible or intangible goods or rights that have monetary value, and any kind of legal documents or instruments certifying rights on them (ROM, art.3). While no explicit provision exists as to whether the ML offence could extend to assets acquired indirectly, provisions that enable corresponding or equivalent value confiscation (TCL, art. 54, 55 and 282) in addition to cases provided seem to cover this.

Criterion 3.5

When proving that property is the proceeds of crime, there is no requirement that a person be convicted of a predicate offence. Instead, it must simply be proven that the property has been acquired as a result of an offence (TCL, art. 282(1)).

Criterion 3.6

There is no explicit provision in the TCL that predicate offences extend to conduct that occurred in another country when this constitutes an offence in that country. Turkish courts have jurisdiction over ML offences committed whether in a foreign country or within Türkiye (TCL, arts. 11 – 13). The law does not distinguish between predicate offence committed outside or inside Türkiye (TCL, art. 282). Türkiye provided a court case to confirm that this is covered.

Criterion 3.7

The ML offence applies to any person, including those who commit the predicate offence TCL, art.282(1), as the TCL does not preclude the perpetrator of the predicate offence from being charged with self-laundering when the acts are related to conducting an act for the purpose of concealing or disguising the illicit origin. The law explicitly states that purchasing, accepting, possessing or using illicit funds constitutes a ML offence for third-party launderers (TCL, art.282(2)), and for self-launderers based on the art.282(1) it would be possible when this is conducted with the specific intention of disguising or concealing the illicit source of funds.

Criterion 3.8

Türkiye provided case examples, whereby intent and knowledge required to prove the ML offence could be inferred from objective factual circumstances. The existence of a criminal offence depends upon the presence of intent. Intent is defined as knowingly and willingly conducting the elements in the legal definition of an offence. There is probable intent when the individual conducts an act while foreseeing that the elements in the legal definition of an offence may occur (TCL, art. 21(2)).

Criterion 3.9

Natural persons are subject to imprisonment of between three and seven years and judicial fines[50] for up to 20 000 days for ML and predicate offences (TCL, art. 282(1)). ML sanctions for acts mentioned in art. 282(2) ranged from two to five years. Statutory sanctions may be increased for aggravating circumstances (TCL, art. 282(3) and (4)). Imprisonment is increased by 50% if the ML offence is committed by a public official or any professional in the course of performing his or her duty and may be doubled if committed by an organised criminal group. These sanctions are considered dissuasive.

Criterion 3.10

When a legal person is involved in the commission of an ML offence, it is subject to specific security measures (TCL, art.282(5)), such as the cancelation of its license and confiscation measures. No criminal penalties shall be imposed on legal persons (TCL, art.20 (2)), as implementation of criminal measures against legal persons is contrary to the fundamental principles of the criminal justice system in Türkiye, according to authorities. In addition to security measures, legal persons that are misused for the commission of an ML offence are also subject to administrative fines - which range from EUR 2 071 – EUR 10 356 100 – but the fine cannot be less than the double amount of the benefit subject to action or activity (Law 5326, art. 43/A). This administrative fine shall be increased yearly according to the Tax Procedure Law (Law No. 213, art. 298). These administrative fines are considered proportionate and dissuasive.

Criterion 3.11

Ancillary offences are criminalised, through general prohibitions relating to participation, conspiracy, attempt, assisting, facilitating and counselling, as well as incitement and assistance to the commission of an offence (TCL, arts. 35 to 41). However, aiding and abetting are not criminalised.

> ***Weighting and conclusion –*** The main shortcomings include the definition of ML as being not totally in line with the Conventions as the act of concealing and disguising assets requires a specific intention, a minor shortcoming with regard to self-money laundering. Recommendation 3 is rated **largely compliant.**

Recommendation 4 – Confiscation and provisional measures[51]

In its 2019 MER, Türkiye was rated compliant with R.4. Türkiye is now being assessed pursuant to changes to R.4 on establishing asset recovery as a policy and operational priority, requiring countries to establish non-conviction based confiscation regimes in their legal system to the extent consistent with fundamental principles of domestic law, implement extended confiscation, the provision of the power to suspend or withhold consent to transactions and freeze and seize expeditiously; recognition of other countries preliminary and final court orders and implementation of informal co-operation mechanisms in the context asset recovery.

General principles

Criterion 4.1

Sub-criterion 4.1 (a)- has policies and operational frameworks that prioritise asset recovery in both the domestic and international contexts.

[50] A judicial fine is an amount payable to the State Treasury by the offender, which is calculated, unless otherwise stated in the law, by multiplying the identified number of days, which shall be more than five but not more than seven hundred and thirty, with a daily amount: TCL, art.52. The daily amount of the judicial fine is, at least, one hundred Turkish lira or, at most, five hundred Turkish Lira and is determined having regard to the personal and economic conditions of the person.

[51] Recommendation 4 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

At a policy level, the Judicial Reform Strategy Document is the highest-level guidance document on judicial matters and includes strategic objectives on the importance of seizing, confiscating and implementing all legal and administrative measures in ML, associated predicate offences and TF offences for asset recovery purposes. It also outlines the prioritisation of establishing an institutional structure to make the necessary arrangements for the identification, confiscation and management of the proceeds of crime by examining international examples (Judicial Reform Strategy Document 2009, updated in 2015 and 2019; strategic objective 3.1(d), 3.2(i)).

In line with this strategic objective, MASAK's AML/CFT strategy also emphasises the importance of depriving criminals of their proceeds as a key element of the fight against financial crimes and set up the need for a legislative framework and effectiveness assessment aimed at prioritising the seizure of the proceeds of and confiscation of values in the context of ML, associate predicate offences and TF (Strategy Document for increasing AML/CFT and Confiscation Practices in Türkiye- 201/2025- Strategic Priority 4.1; PD 2021/16).

At an operational level, Türkiye's General Directorate of Criminal Affairs issued a circular (Circular No. 155/1) applicable to all prosecutors noting the importance of prioritising the implementation of seizure and confiscation orders when conducting ML/TF investigations. This Circular also encourages parallel financial investigations in line with national risks, applying security measures and administrative sanctions for legal persons in case of ML or TF, examining whether assets were taken abroad in ML and TF offences, and ensuring specialisation in the conduct of investigations which all contribute overall to Türkiye's national policy on asset recovery.

In addition, in line with its Judicial Strategy Document (2021-2025), Türkiye has set specific criteria for the various institutions involved in pursuing the recovery of assets, confiscations and the management of assets in order to clarify areas of responsibility and establish measurable performance criteria. Türkiye's Co-ordination Board for Combatting Financial Crimes (CBCFC) plays a central role in ensuring co-operation and co-ordination among relevant institutions within the AML/CFT regime. This includes the development of strategies and mechanisms to enhance the effectiveness of asset recovery efforts, evaluating draft legislation on the prevention of ML/TF, strengthening co-operation between institutions and organisations in the implementation process, determining implementation strategies and making policy decisions in this regard (Presidential Decree No. 1 art.232). In accordance with MASAK's strategic objectives, Türkiye has also created three working groups (Threat Working Group, Vulnerabilities Working Group and Sanctions Monitoring Working Group), and numerous sub-working groups have been established which meet regularly, as deemed necessary, to monitor progress and address challenges at an operational level. Their mandate specifically requires the periodical collection of statistical data on seizure and confiscation and annual evaluation by the Threat Working Group to assess and further improve Türkiye's asset recovery regime. LEAs, judicial authorities, MASAK and other relevant competent authorities are members of the before-mentioned Threat Working Group (Strategy Document for Increasing AML/CFT and Confiscation Practices in Türkiye, Activity 4.1.b). Moreover, the National Judiciary Information System displays an indicator as to whether seizure and confiscation measures have been applied and keeps record of all information related to the seized assets, along with their determined values.

In 2024, Türkiye established seven court houses for International Judicial Co-operation in Criminal matters to pursue judicial co-operation effectively and quickly with the aim of promoting international co-operation for asset recovery purposes (Circular No.183). In addition, public prosecutors are requested to investigate whether the proceeds have been transferred/moved abroad in the context of an ML/TF and associate predicate offences investigation (Circular 155/1).

Sub-criterion 4.1 (b)- has created three working groups and numerous sub-working groups which meet regularly as deemed necessary (in practice, 3 to 4 times a year since 2021) to monitor progress and address challenges identified, including in asset recovery policies and its operational implementation (see

description in the above subcriterion). The Threat Working Group is specifically required to periodically collect statistical data on seizure and confiscation annually and to assess and further improve Türkiye's asset recovery regime. The Threat Working Group is integrated by the main AML/CFT competent authorities, including LEAs, judicial authorities, MASAK and other relevant competent authorities with the objective of embedding operational asset recovery findings into national policies (Strategic Document for Increasing Effectiveness in AML/CFT and Confiscation Practices in Türkiye- 2021/2025- Activity 4.1.b).

The CBCFC meets twice a year and periodically reviews Türkiye's national asset recovery regime to ensure its ongoing effectiveness. For this purpose, the Directorate General for Criminal Affairs periodically holds evaluation meetings accompanied by the Public Prosecutors assigned at the investigation's bureau of laundering offence (Circular 155/1) where they discuss the operational impact of the asset recovery policies. Furthermore, inspectors from the Ministry of Justice regularly supervise the related proceedings (Regulation on Property of Crime, art.28). During this process, they check whether the provisions of this Regulation and other relevant Regulations are complied with in the proceedings of taking, keeping, returning the criminal property, and their confiscation and liquidation.

Sub-criterion 4.1(c)– Provides sufficient resources to effectively pursue asset recovery. Türkiye's public prosecutors investigate all crimes, including ML, related predicate offences and TF (CPL, art. 160-169) and they carry out this duty directly or through LEAs (TNP, GGC, Customs Enforcement and the Coast Guard) (CPL, art. 164(1)). LEAs have special ML units with a total of 1371 trained officials in asset recovery processes aimed at increasing the effectiveness of Türkiye's investigations and asset recovery efforts. MASAK, the Banking Regulation and Supervision Agency (BRSA), Capital Markets Board (CMB), Ministry of Treasury and Finance (MoTF), and/or the Public Oversight, Accounting and Auditing Standards Authority are contributing to the asset recovery process with their expertise, which includes the identification, tracing and evaluation of the property subject to seizure (CPL, art.128).

In relation to management of the seized assets, when the administration of seized immovables, rights, and credits is necessary, a trustee may be appointed for the administration of these assets (CPL, art. 128/10). Savings Deposit Insurance Fund (SDIF) can be assigned by the court as a trustee for up to five years (Law No. 7539 published in the Official Gazette on February 4, 2025). This applies in cases where there is strong suspicion that the crimes of laundering assets derived from crime and TF, as defined in the TCL and the TF Law, have been committed. The regulation also includes provisions for the management of these assets, the protection of their value and their sale, if necessary (CPL, art.133).

Sub-criterion 4.1(d)- has a legal and institutional framework in place to enable effective use of the asset recovery regime, consistent with R.2. The Board for Combating Financial Crimes chaired by MoT, ensures co-operation and co-ordination among relevant institutions within the AML/CFT regime including asset recovery matters. When necessary, representatives of institutions and organisations may be invited to the Co-ordination Board meetings for their opinions and information. The Co-ordination Board shall convene at least twice a year. Türkiye has also established special ML units within LEAs to increase the effectiveness of investigations and asset recovery efforts. A depository bureau is available in every province and district where a Prosecutor's Office and Chief Public Prosecutor's Office is available to better co-ordinate ML, associate predicate offences and TF investigations, including asset recovery processes. In the International context, Türkiye has established 7 courthouses to carry out international judicial co-operation procedures effectively and quickly ("Offices for International Judicial Co-operation in Criminal Matters" 4th Strategy Document on Judicial Reform, obj. 1.17 (c)).

Investigative measures

Criterion 4.2

Türkiye has measures, including legislative measures, that enables their competent authorities to:

Sub-criterion 4.2 (a)- identify, trace and evaluate criminal property and property of corresponding value. Public prosecutors can search a suspect or accused person based on reasonable suspicion of their involvement in a crime (CPL). If there are cases that allow to assume that the person sought, or the evidence of the crime is in the specified places, other people, belongings, homes, workplaces or other places belonging to them may also be searched. Items, found during the search are seized and their value is determined. LEAs can conduct such operations under the delegation of the Public Prosecutor in relation to evaluation identification and tracing, expertise may also be specified among the mechanisms of determining the assets which are subjected to confiscation or suspected to be derived from proceeds of crime (CPL, art. 63). In relation to the evaluation of criminal property and property of corresponding value, it is compulsory to determine the value of all assets under government protection or those that have been seized (CPL, art.123(3)) and to record all information related to the seized assets, along with their determined values (Regulation on Property of Crime, art. 5(3)). Furthermore, prior to seizure, MASAK, the Banking Regulation and Supervision Agency (BRSA), Capital Markets Board (CMB), Ministry of Treasury and Finance (MoTF), and/or the Public Oversight, Accounting and Auditing Standards Authority are contributing to the asset recovery process with their expertise, which includes the identification, tracing, and evaluation of the property subject to seizure. (CPL, art.128).

Sub-criterion 4.2 (b)- take any other appropriate investigative measures. Public prosecutors can request the following investigative techniques:

a) Detection of communication, wiretapping and record of communication (CPL, art.135)
b) Assignment of undercover investigators (CPL, art.139)
c) Surveillance with technical devices (CPL, art.140)
d) Controlled delivery (Law No 4208, art. 2, 10, 11 and 13)

All these techniques are applicable for ML (AML Law 17(3)) and TF investigations (TF Law, art. 4(8).

Provisional measures

Criterion 4.3

Sub-criterion 4.3 (a): has measures, including legislative measures, which enable MASAK and/or and LEAs, in response to relevant information, to take immediate action, directly or indirectly, to withhold consent to or suspend a transaction suspected of being related to ML, a predicate offence, and TF. The Minister of Treasury and Finance is authorised to suspend the transactions that are either attempted or currently ongoing within or through obliged parties for a period of seven working days. During this time, MASAK (Financial Crimes Investigation Board) is tasked with verifying the suspicion, analysing the transaction, and, if necessary, conveying the results of its analysis to the competent authorities (AML Law, art. 19/A). The Minister may delegate this authority. Postponement of transactions can be triggered in the following:

a) upon the request of the obliged parties (AML Law, art. 4)
b) ex-officio by MASAK (AML Law, art. 5)
c) upon requests received from foreign competent authorities. (AML Law, art. 6)

Sub-criterion 4.3 (b)- The maximum duration of this measure is specified as seven working days, which allows sufficient time for MASAK to analyse the transaction and for competent authorities to initiate appropriate actions, such as freezing or seizing the assets. Moreover, this measure can be renewed if deemed necessary, ensuring that competent authorities have adequate time to complete their analysis and take further action if required (AML Law, art. 19/A, Regulation on Postponement of Transactions within the Scope of Prevention of Laundering Proceeds of Crime and Financing of Terrorism).

Criterion 4.4

Türkiye has measures, including legislative measures, to enable their competent authorities to expeditiously carry out provisional measures. This should include:

Sub-criterion 4.4 (a)- freezing and seizing measures to prevent any dealing, transfer or disposal of criminal property and property of corresponding value. Türkiye allows the search conducted to collect criminal evidence (CPL, art.116-122) and seize the assets, which are considered as means of evidence, or which is the subject of confiscating the materials and the earnings (CPL, art.123-134). In cases where delay is prejudicial the senior law enforcement officer can take the search measure (CPL, art.119). Assets which are deemed useful as a means of proof, or which constitute the subject matter of confiscation of property and proceeds of crime (including corresponding value) are to be taken under protection. If they are not surrendered voluntarily, they shall be seized. (CPL, art.123).

Sub-criterion 4.4 (b)- As elaborated in detail in 4.4 (a), none of the searching and seizing provisions stipulated in articles 116-134 of the CPL include a requirement to inform or give notice in advance of the freezing or seizing of criminal property and property of corresponding value.

Sub-criterion 4.4 (c)- ensuring that provisional measures do not have unreasonable or unduly restrictive conditions for effective action, such as in relation to demonstrating the risk of dissipation. The seizure order is to be taken by the judge. Immovables, rights and credits can be seized (CPL art. 128). However, in cases where delay is prejudicial, the public prosecutor can take this measure. In addition, if he/she cannot be reached and delay is prejudicial, the senior law enforcement officer can also take this measure to expeditiously deprive these assets (CPL, art. 119 and 127). However, in ML and TF where delay is prejudicial, the public prosecutor can also take this measure (AML Law, art. 17) and take the decision to the judge on duty for approval. The judge will decide on whether it will be approved or not in twenty-four hours at the latest.

Criterion 4.5

As referenced in 4.4 (c), Türkiye allows public prosecutors and LEAs to freeze and seize criminal property and assets which are deemed useful as proof including property of corresponding value (CPL, art. 123) without a court order when it is necessary to act expeditiously and where delay is prejudicial to the process (see 4.7 below). These orders shall be then reviewed and homologated by a judge.

Criterion 4.6

Türkiye has measures, including legislative measures, that enable competent authorities to take steps that will prevent or void actions that prejudice the country's ability to freeze, seize or confiscate criminal property and property of corresponding value. FIs are informed immediately about the seizure order to seize the account they hold, and acts conducted after such order which aim to thwart the dispossession are void (CPL, art. 128(5)). Those who act against the seizure order can be imprisoned up to three years and applied judicial fine 1.500.000 TRY (approx. 42.000 EUR) (CPL, art. 128(8)). The Minister of Treasury and Finance is authorised to suspend the transactions that are either attempted or currently ongoing within or through obliged parties for a period of seven working days. During this time, MASAK (Financial Crimes Investigation Board) is tasked with verifying the suspicion, analysing the transaction, and, if necessary, conveying the results of its analysis to the competent authorities (AML Law, art. 19/A). The contracts between the parties which aim to prejudice the country's ability to freeze, seize or confiscate are not binding the court (excluding the property or the gains which belong to bona fide third parties). Even if the contract itself is valid in respect of civil law, criminal court may remove legal effect of this contract (Law No 6098, Art. 19). The legal contracts including unlawful provisions regardless of whether they are based on an agreement are invalid and ineffective with regard to law.

Confiscation

Criterion 4.7

Türkiye has measures, including legislative measures, to enable the confiscation of criminal property and property of corresponding value after a person is convicted. Criminal property deriving from ML, predicate offences and TF is to be confiscated (TCL, art. 54(1) and 55(1)). Following the notification of the confiscation decision by the criminal courts, the tax administrations will commence the collection of receivables by issuing a written notice (Law No. 6183, art. 37) granting a one-month payment period. If the amounts are not paid within this period, an extra fee shall apply (Law No. 6183, art. 51).

Depending on the type of assets subject to confiscation, the officer will issue a payment order for the defendant to deposit the equivalent cash (Law No. 6183, art.55), with the documents stating the receivables and ownership rights for movable and immovable property (Art. 62) or any other assets (art. 77). The confiscated assets shall be appraised by the officer who seized them (art. 81). Upon the debtor's request or if deemed necessary by the collection office, the valuation of the assets can also be conducted or reviewed by an expert witness (valuation experts) pre-vetted by the MoJ. The valuation report shall be presented to the MoTF to decide on the confiscated asset management, selling or liquidation if needed (Law No. 6183, art. 81-91 and Law No. 6754, art. 6).

In cases where it is not possible to seize or confiscate the property subject to confiscation or the criminal property is not handed over, property of corresponding value shall be confiscated (TCL. art. 54(2) and 55(2)). In cases where the assets or material benefits subject to confiscation cannot be seized or delivered to the competent authority, a copy of the final decision concerning the confiscation of their corresponding value shall be sent directly by the court to the chief revenue officer of the location where the decision was rendered (Law No. 6183 on the Procedure for Collection of Public Receivables).

Criterion 4.8

Türkiye's legal framework prohibits general confiscation pursuant to Article 38(9) of the Constitution and does not allow confiscation to be extended to assets derived from criminal conduct other than the offence(s) underlying the conviction. As such, Türkiye does not provide for extended confiscation based on a presumption of criminal origin linked to broader criminal activity. Türkiye applies a post-conviction confiscation mechanism whereby additional property of a person previously convicted of ML, predicate offences or TF may be confiscated if newly discovered assets are demonstrated to be proceeds or instrumentalities of the offence subject to the prior conviction. This requires the initiation of a separate confiscation proceeding (CPL, Article 256(2)), supported by a financial investigation and judicial determination. In such proceedings, the court's assessment is limited to determining whether the newly identified assets constitute proceeds or instrumentalities originating from the criminal conduct underlying the previous conviction.

Criterion 4.9

Türkiye has measures, including legislative measures, to enable the confiscation of criminal property without requiring a criminal conviction (non-conviction-based confiscation) in relation to a case involving ML, predicate offences or TF, only in limited cases and in line with their fundamental principles of domestic law.

According to Türkiye's TCL, to be able to apply the confiscation measure it is necessary for an object or gain to be used in an offence, obtained following the commission of an offence or assigned for the commission of an offence which is determined through a conviction according to the fundamental principles of domestic law. However, non-conviction based confiscation (NCBC) is possible on the condition that the property does not belong to any third party acting in good faith, if the property that is prepared for the purpose of committing a crime presents a danger to public security, health or morality (TCL, art.

54(1)); an amount equal to the value of the property can be confiscated if the property cannot be confiscated because it has been destroyed, given to another, consumed or, for any other reason (TCL. art. 54 (2)); and for any property where the production, possession usage, transportation, buying and selling of which has constituted an offence and where the perpetrator is unknown (TCL, art. 54(4)):

In case of death of the accused: trial regarding the objects and material benefit subject to confiscation based on their nature shall be carried on and their confiscation may be ordered. (TCL, art. 64(1)).

In case the accused, whose whereabouts are not known, or who is abroad and cannot be brought in, or it is not appropriate to bring him before the competent court, is considered as an absentee. The law does not allow opening a hearing against these individuals but allows carrying out the necessary proceedings with the aim of obtaining or protecting evidence. Therefore, it is possible to apply the seizure measure regarding any property that may be subject to confiscation within the framework of the general provisions.

In case the accused is a fugitive and with the aim of bringing the fugitive to justice, their belongings located in Türkiye and his rights and accounts receivables may be seized. As a result of the fact that the fugitive accused persons are aware of the case against them opposed to the defaulters, it is possible to seize all assets of the fugitive.

Even if it is not possible to convict a person due to some reasons (e.g. minority and mental illness), the court may render a decision for confiscation.

Asset recovery and tax authorities

Criterion 4.10

With a view to enhancing asset recovery efforts and supporting the identification of criminal property, Türkiye has signed protocols for information sharing and co-operation between their competent authorities (MASAK, LEAs and Prosecutors Offices) and the TRA. In 2024, a protocol on data sharing was signed between the TRA and MOJ to access the information in the TRA database in a secure environment through UYAP within the scope of investigation and trial activities. In 2025, Türkiye implemented software for querying banking deposit/portfolio identification information through UYAP. This allows judges and public prosecutors to request personal banking information (TR ID No, Tax ID No, Name-Surname, Bank name, Branch name, IBAN / Account No, Account Type, Currency, Account Partnership Status, Account Partnership Percentage, Account Status, Date fields are included) and information on which bank or banks the person has an account.

Asset management, return and disposal

Criterion 4.11

Türkiye has mechanisms to manage and, as necessary, dispose of frozen, seized and confiscated property, according to the Regulation on Property of Crime. In addition, when there is a likelihood that a seized item will be damaged or suffer a substantial loss of value, the item in question may be liquidated before final judgment (CPL, art.132). In other cases when there are strong grounds of suspicion that the crime is being committed, within the activities of a firm, and it is necessary to reveal the true state of affairs, the judge or the court is entitled to appoint a trustee for the administration of the firm. (CPL, art. 133). A depository bureau is available in every province and district where a Prosecutor's Office and Chief Public Prosecutor's Office is available.

For asset management, a trustee may be appointed for the administration of the seized immovable, rights and credits, when necessary (CPL, art. 128/10) and the Saving deposit insurance fund (SDIF) can be assigned by the court as a trustee for up to 5 years under law 7539. This applies in cases of ML/TF. According to the

Regulation on Property of Crime, the mechanism used for the management and disposal of property includes, but is not limited to, the following:

a) Establishing a depository, supervision and monitoring of procedure (art. 4).
b) Preservation and seizure of property of crime (art. 5).
c) Preservation of Properties of Crime (art. 8).
d) Procedures to be carried out regarding valuable properties and documents, and properties of crime that can be damaged or can lose value or which are hard to preserve (art. 10).
e) Procedures for land, air and sea vehicle (art. 12).
f) The process of depositing money into the bank (art. 14).
g) Principles relating to money deposited in banks (art. 15).
h) Procedures, related to a property of crime, which is decided to be returned or disposed of, before the finalisation of such order (art. 16).
i) Procedures, related to properties of crime, for which confiscation or return-to-owner orders are given (art. 17).
j) Procedures for the execution of confiscation and return decisions on non-circulating money as well as the value of assets that constitute the subject of the confiscation of property of crime and earnings (art. 18).
k) Procedures concerning the confiscation and reimbursement of the money deposited in a bank (art. 19).
l) Procedures to follow regarding the property that is not taken by its owner or the owner of which is anonymous (art. 21).
m) Sale procedures (art. 22).
n) Property of crime owned by absent or deceased persons (art. 23).
o) Disposal of the property which does not have any value (art. 24).
p) Liquidation of the property in the deposit with no connection to the relevant entry of property of crime (provisional[52], art. 1).

Criterion 4.12

Türkiye has measures that enable them to enforce a confiscation order and realise the property or value subject to the confiscation order, leading to the permanent deprivation of the property or value subject to the order. All other property (movable, immovable and all other goods) which are decided to be confiscated are delivered to the highest ranked property office of the province/district or to the relevant departments.

In cases where the property or material benefits subject to confiscation cannot be confiscated or delivered to the authority, the finalised copy of the decision on the confiscation of the corresponding value is directly submitted by the court to the highest ranked property officer of the place where it is located, and the execution is carried out (Law on Collection Procedure of Public Receivables numbered 6183). The realisation of confiscated property is carried out through established procedures based on the principles of public welfare, transparency and accountability. Confiscated properties by court order are handed over to the relevant public institution, the properties are examined if they can be used for public services, either eligible or to be sold. The sale is carried out by auction or negotiation in accordance with the provisions of the state procurement law (Law No. 5018, art. 45, 46). Movable cultural and natural assets seized due to offences within the scope of Law No. 2863 on the Conservation of Cultural and Natural Property shall be delivered to the museum.

[52] Provisional articles are a common practice in Turkish legal system. These provisions are regulatory texts that begin at the end of the main provisions in the text of the law and generally contain procedural provisions relating to enforcement and implementation.

Criterion 4.13

Sub-criterion 4.13 (a) (Met)- has a mechanism to return property and funds to its prior legitimate owner/ victim of the offence if this is a natural or legal person (Law No. 5271, art. 131). If the property cannot be returned, it is then confiscated (TCL, art. 54 and 55).

Sub-criterion 4.13 (b) (Mostly Met)- can use confiscated property to compensate victims of crime in some but not all offences: in TF cases (Law No 5233, art. 7). Türkiye also has the "effective remorse" provisions which allow victims who have suffered material damage or whose personal rights have been violated due to the offence to claim compensation for the damages they have suffered through a compensation lawsuit to be filed in civil courts (TCL, art. 168 for offenses against property, art. 248 for embezzlement offence, and art. 254 bribery offence). For the remaining offences according to Türkiye's budgeting principles all government revenues and expenditures should be included in a sole budget, therefore there are no specific revenues to specific expenditures (Law No. 5017, art. 6). Notwithstanding these funds can and have been used to fund rehabilitation and other purposes (e.g. in case of victims of narcotics/drug trafficking cases).

> ***Weighting and conclusion –*** Türkiye has robust confiscation and provisional measures and mechanisms where asset recovery is prioritised at policy and operational levels. Competent authorities have the legal and institutional framework and mechanisms to identify, trace and take any appropriate investigative measures to confiscate and apply provisional measures. However, extended confiscation does not extend to conduct other than that previously subject to conviction and property of corresponding value and asset returns to victims is limited to TF, fraud and those victims that suffered material damage in offences against property, embezzlement and bribery. Recommendation 4 is rated **largely compliant.**

Recommendation 5 – Terrorist financing offence[53]

In its 2019 MER, Türkiye was rated largely compliant with R.5 because sanctions for TF for legal persons (administrative fines) were not dissuasive.

Criterion 5.1

TF criminalisation in Türkiye is consistent with art. 2 of the TF Convention. Türkiye criminalises the wilful provision and collection of funds when there is intention that funds are used, or with the knowledge that they are to be used, in full or in part, in perpetration of acts listed within art.3[54] : TF Law, art.4).

Criterion 5.2

The TF offence in Türkiye extends to any person who provides or collects funds for a terrorist or terrorist organisation, with the intention that they are used, or knowingly and willingly are to be used, even without being linked to a specific act, in full or in part in perpetration of the acts that are set forth as a crime within the scope of art. 3 (TF Law, art.4). Court cases confirm that art. 4, in particular the mental element of the TF offence, does not require the intention that a specific terrorist act be committed.

[53] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits (adjust numbering of criteria in line with FATF Methodology).

[54] This includes acts i) intended to cause death or serious bodily injury for the purpose of intimidating or suppressing a population or compelling a government or an international organisation to do or to abstain from doing any act; ii) acts set forth as terrorist offences in Anti-Terror Law; and iii) acts that constitute an offence, as defined in the Annex to the TF Convention.

Criterion 5.3

Türkiye criminalises the preparation of terrorist acts: TCL, art. 39 and TF Law (TF Convention, art.2). The wording of these offences and the application in the court appears to cover the case where travel has been financed.

Criterion 5.4

The TF offence applies to funds covering money or property, rights, claims of every kind whether movable or immovable, tangible or intangible, which could be represented by money and all kinds of documents representing them: TFL, art.(2)(1)(c). Türkiye makes a distinction between financial support and non-financial support. The TF offence covers cases when the value of financial support can be measured. In other cases, where non-financial support is provided (e.g. the provision of transportation), the general provisions of the TCL would be applied, as assistance to a terrorist organisation: TCL, art. 220(7). Regarding the source of the funds, the definition does not distinguish between legitimate or illegitimate sources.

Criterion 5.5

The TF offence does not require that the funds were actually used to carry out a terrorist act or were linked to a specific terrorist act. It is sufficient that it is intended or reasonably suspected that the funds could be used for this purpose (TFL, art.4). In addition, the Court of Cassation of Türkiye confirmed interpretation of TF criminalisation, in particular the mental element of the TF offence, which does not require intention that a specific terrorist act be committed.

Criterion 5.6

Intent and knowledge required for the commission of a TF offence can be proved in Türkiye by relying on objective factual circumstances (TCL, art. 21). Cases provided confirmed this (Court of Cassation, the Ninth Penal Chamber of the Court of Cassation Date 22.05.2013, Decision No 2013/8053, Case No. 2013/3017).

Criterion 5.7

Natural persons convicted of a TF offence are subject to terms of imprisonment from five to ten years. These sanctions are considered as dissuasive and proportionate. Aggravated sanctions are available in relation to these terms of imprisonment depending on the other circumstances of the offence.

Criterion 5.8

When the TF offence is committed within the framework of a legal person's activity, the legal person is subject to specific security measures, such as the cancelation of its license and confiscation measures (TF Law, art. 4 (5)). No criminal penalties shall be imposed on legal persons (TCL, art.20 (2)) as implementation of criminal measures against legal persons is contrary to the fundamental principles of the criminal justice system in Türkiye, according to authorities. In addition to security measures, legal persons that are misused for the commission of a TF offence are also subject to administrative fines, which range from EUR 2 071 – EUR 10 356 100, but the fine cannot be less than the double amount of the benefit subject to action or activity (Law 5326, art. 43/A). These administrative fines are mostly proportionate and dissuasive.

Criterion 5.9

Ancillary offences are covered in the general provisions of the TCL. These include attempt to commit TF (art.35), participation as an accomplice (art.37), soliciting another person to commit TF (art.38) and acting in common purpose[55] (art.220).

Criterion 5.10

The TF offence is a ML predicate offence due to the sentencing regime as well as the fact that the TF offence carries more than a six months' imprisonment threshold.

Criterion 5.11

Türkiye has legislation in place to deal with persons alleged to have committed a TF offence in the same or different country from where the terrorist individual or terrorist organisation is located, where the acts occurred or where the acts would occur.

> *Weighting and conclusion –* Türkiye has minor shortcoming as the sanctions applied to the legal persons for TF offence is mostly dissuasive. Recommendation 5 is rated **largely compliant.**

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing[56]

In its 2019 MER, Türkiye was rated partially compliant with R.6 and re-rated largely compliant in its 2021 FUR.

Identifying and designating

Criterion 6.1

a) The President of the Republic of Türkiye (referred to as "the President") is the competent authority with responsibility for proposing persons or entities to the 1267/1989 Committee for designation, and for proposing persons or entities to the 1988 Committee (Law 6415, art. 5(4)). These decisions are to be transmitted to the relevant UNSC by the Ministry of Foreign Affairs (Law 6415, art. 5(4)).

b) Türkiye has a mechanism for identifying targets for designation on its own initiative in line with UNSCRs 1267/1989 and 1988 (Law 6415, art. 5 and RoTF, art. 4/A). In this framework, upon suggestion of the Assessment Commission (AC), the President may suggest the United Nations Security Council to list relevant individuals, entities or organisations pursuant to relevant UNSCRs (Law 6415, art. 5(4)). The AC is under the chairmanship of the head of MASAK and is composed of representatives from MASAK, National Intelligence Agency, Ministry of Interior, Ministry of Justice, Ministry of Foreign Affairs, Ministry of Treasury and Finance (RoTF, art. 9). Representatives from other institutions may also be invited if deemed relevant.

   The secretariat duties of the AC are carried out by MASAK (RoTF, art 9(5)) which also receives the information from all competent authorities regarding potential designees (RoTF, art 4/A(1)). MASAK can also trigger this process at its own motion and thereafter prepares a financial research

[55] According to TCL, art. 220, if three or more people found an organisation in order to commit a crime, the founders and administrators of this criminal organisation are to be imprisoned from 2 to 6 years and those who become a member of the organisation are to be imprisoned from 1 to 3 years. In cases where the organisation is armed the penalties applied are increased from ¼ to ½.

[56] Recommendation 6 is newly assessed due to changes (implementation) changes that were not assessed during Türkiye's mutual evaluation and follow-up report.

report on the potential designees, which is then submitted to the AC for further consideration (RoTF, art. 4/A(2)).

AC's review of the case is written in to a minute which together with the financial research report prepared by MASAK is then forwarded to the President, which decides whether there are reasonable grounds for designation (RoTF, art 4/A(1)).

c) Türkiye applies an evidentiary standard of proof of "reasonable grounds" (Law 6415, art. 5(4)).

d) Türkiye follows the procedures and, in the case of UNSCRs, the standard forms for listing, as adopted by the relevant committees when acting as a cosponsor at the request of another jurisdiction. (the 1267/1989 Committee and 1988 Committee).

e) Türkiye has the legal framework to provide as much relevant information as possible.

Criterion 6.2

a) The President of the Republic of Türkiye is the competent authority with responsibility for designating person or entities upon the request of another country (Law 6415, art. 6 and RoTF, art.5). Whereas, in cases of domestic designation at the country's own initiative, this responsibility belongs to the Minister of Interior and Minister of Treasury and Finance (RoTF, art 7(4)).

b) Türkiye has a mechanism for designating persons or entities that meet the specific criteria for designation, as set forth in UNSCR 1373; as put forward either on the country's own motion or, after examining and giving effect to, if appropriate, the request of another country (Law 6415, art. 7, para. 3). How the process works for designations on its own initiative is that MASAK collects information on potential designees, conducts research and produces a financial research report before presenting proposals to the AC. The AC then presents its meeting minutes to the Minister of Interior and Minister of Treasury and Finance, which will decide whether to domestically designate these persons. On the other hand, incoming foreign requests must be made directly to MASAK, the Ministry of Justice or the Ministry of Foreign Affairs (who then conveys the request to MASAK), for further review (Law 6415, art. 6). The AC considers proposals for designations (Law 6415, art. 9). The AC's recommendations are forwarded to the President, who makes the final determination.

c) As decisions on freezing of assets and repeal of such decisions gain legal validity in Türkiye upon their publication in the Official Gazette (Law 6415, art. 12 (1)), the Department of Administrative Affairs of the Presidency issued an Administrative Order to different ministries and authorities stating that procedures about UNSCRs are to be completed urgently and as soon as possible, in order to reduce the ratification time. Administrative orders made by the President are directly applied by all public authorities and considered as binding and enforceable means by all administrative units.

d) Türkiye applies an evidentiary standard of proof of "reasonable grounds" when deciding whether or not to make a designation (Law 6415, art 7(1) & RoTF, art. 6 (3) and 8 (2)). The designation is not conditional upon the existence of a criminal proceeding, and a designation may be made without the existence of an ongoing criminal proceeding. However, the TF Law allows for an option to annul if the requesting country does not initiate an investigation within one year from publication in the Official Gazette, and there are cases which carry these criteria. To date, Türkiye has not applied this provision. This provision is believed to be helpful in protecting fundamental rights.

e) Türkiye has the legal framework to provide as much information as possible with outgoing requests.

Criterion 6.3

MASAK has the legal authority to collect or solicit information to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation. It also

has the legal authority to operate *ex parte* against a person or entity who has been identified and whose (proposal for) designation is being considered (Law 6415, art 8).

Freezing

Criterion 6.4

For TFS implemented as part of UNSCR 1267 and successor resolutions, MASAK is notified without delay of any update of the list, both directly via the distribution list of the UN and via an official letter from Türkiye's Permanent Representation at the UN. MASAK then transmits the information to the Presidency of the Republic of Türkiye without delay. Once ratified by the President, the listing decision is published in the Official Gazette without delay (RoTF, art. 4). The decisions on freezing of assets and repeal of such decisions gain legal validity in Türkiye upon their publication in the Official Gazette (Law 6415, art. 12 (1)). Even though there is no explicit requirement for the ratification to also take place without delay, this process has occurred without delay during the reporting period in some instances while in others two to four working days were needed for the domestic transposition of TFS obligations under UNSCR 1267. Upon new UN designations, mitigating measures are applied: prior to sending listings decision to the Presidency for ratification, MASAK identifies potential funds or assets and verify possible occurrences or links within Türkiye. If such funds or assets are found, the Minister of Treasury and Finance can postpone the transactions on the targeted funds and assets for seven working days (Law 5549, art. 19/A) even before the formal ratification of the Presidential decree implementing TFS would have occurred. As no matches were found over the reporting period, this mechanism has not been resorted to over the reporting period.

For domestic sanctions, including emanating from requests made by foreign countries, freezing, decisions are implemented without delay following the publication in the Official Gazette (RoTF, art. 5 & 7).

The Department of Administrative Affairs of the Presidency has sent an Administrative Order to different ministries and authorities stating that procedures about UNSCRs are to be completed urgently and as soon as possible, in order to reduce the ratification time. Administrative orders made by the President are directly applied by all public authorities and considered as binding and enforceable means by all administrative units.

Criterion 6.5

a) Türkiye requires that freezing action be executed without delay by all natural and legal persons, once published in the Official Gazette (Law 6415, art. 5 &12(1) and RoTF, art. 14(3)).

b) The obligation to freeze covers all funds or other assets that are owned, possessed or directly or indirectly controlled by the designated person or entity (Law 6415, arts. 2c and 2ç). Funds or other assets that are jointly owned or controlled, directly or indirectly, by designated persons or entities is also covered (RoTF, art. 3.1(h)). This covers the funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities, and the funds or assets derived or generated from funds or assets owned or controlled directly or indirectly by designated persons or entities (Law 6415, art. 2 (1) ç & RoTF, art.14).

c) Türkiye prohibits their nationals and any persons and entities within their jurisdiction, from making financial services available (Law 6415, art 15(2)). Funds are required to be placed within frozen accounts. Türkiye does so by criminalising to willingly provide or collect funds or provide financial services, for the benefit of individuals, entities and organizations about whom decision of freezing of assets has been made, or for entities controlled directly or indirectly by them, or for individuals or entities who act on their behalf or for their benefit, knowing their nature. While the prohibition does not extend to explicitly cover individuals or entities who act on a designated person's behalf in the revised TF Law, in the Turkish Legal System, a person who acts at the direction of someone else, would be naturally acting on this persons' behalf, whether legally or illegally. However, this

criminalisation does not extend to making other related services available to designated persons and entities.

d) Designations are published in the Official Gazette (Law 6415, art. 5(1)) and these decisions shall be deemed notified to the relevant person, institution or organization about whom the decision on freezing of asset has been made upon their publication in the Official Gazette (RoTF, art. 12(1)). MASAK should inform competent authorities as well as natural and legal persons to whom notification is deemed necessary (RoTF, art. 14). Decisions are communicated through fax, email and web services. MASAK also makes use of an e-notification system when communicating decisions with banks and most FIs (Law 5549, art. 9/a). Clear guidance to FIs and other persons or entities, including DNFBPs that may be holding targeted funds or other assets, on their obligations to take freezing action is available from MASAK.

e) Natural and legal persons, as well as public institutions and organisations, are required to inform MASAK of any "asset records" within 7 days, upon the notification of the freezing decision (Law 6415, art. 12(5) & RoTF, art. 14(2) & (3)). In addition, designated individuals and entities are required to inform MASAK of "claims or debts and all other asset[s]", and natural and legal persons who are in claim or debt relationship with those about whom decision on freezing of asset has been made shall also inform MASAK of the amount of the claim or debt within 30 days of publication of the freezing decision in the Official Gazette (Law 6415, art 12(3)).

f) The rights of bona fide third parties acting in good faith are protected (Law No. 6415, art. 10 and RoTF, art. 13(2)).

Criterion 6.6

a) De-listing requests made to MASAK are to be forwarded to the UNSC through the Ministry of Foreign Affairs (Law 6415, art. 5(3) and RoTF, art. 4(4). The freezing decision should also contain legal remedies and delisting requirements that must be met for an individual or entity to be delisted (RoTF, art. 12(2). General principles of administrative law provide for recourse to judicial review for individuals and entities affected by actions and acts of the administration, including legal recourse for designated individuals and entities (Constitution, art. 125).

b) In addition to general provisions under the Constitution, which allow for aggrieved parties to approach the administrative court of first instance for judicial review, the AC is required to assess in a six-months period whether a listed individual or entity continues to meet the criteria for designation pursuant to UNSCR 1373 (RoTF, art 7(7)).

c) With regard to designations pursuant to UNSCR 1373, the Ministries of Treasury and Justice, who decides on the freezing, shall submit their decision to Ankara High Criminal Court determined by the Council of Judges and Prosecutors within 48 hours following the publication in the Official Gazette (RoTF, art. 7(4)). The court decides to repeal the asset-freezing decision after examining the existence of reasonable grounds (RoTF, art; 7(5)). In addition, relevant persons can make a request for repealing the freezing decision to the Assessment Commission. The AC assesses the request, and the rejected requests shall be forwarded to the Court for final decision (RoTF, art. 7(9)).

d) The Council of State deals with administrative cases related to the annulment of decisions of the President and Ministers in its capacity as the administrative court of first instance. Listed individuals and entities can bring an action for annulment and/or full remedy action before the Council of State within 60 days after the notification of designation. There are no clear procedures to facilitate review by the 1988 Committee, in accordance with any applicable guidelines or procedures adopted by the 1988 Committee, including those of the Focal Point mechanism established under UNSCR 1730. Türkiye does provide a notice to affected designees informing them of their ability to apply to the UNSCR 1988 Committee and mentioning the existence of the 1730 Focal Point; although, it does not say how to do this or for what.

The freezing decisions, which are to be conveyed to the designee's address as well, include the reasons, scope, duration and legal remedies that can be applied against this decision and the application period (RoTF, art 12(2). Furthermore, the "Guidance for Applications Against Freezing Decisions" provides detailed information and forms which can be used to seek review by the 1988 Committee, apply for the de-listing petition to the Office of the Ombudsman and any other application to the United Nations Security Council.

e) Designated persons and entities are informed of this availability. Türkiye does provide a notice to affected designees informing them of their ability to contact the UN ombudsman (Please also see c.6.6.d).

f) Requests to unfreeze funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), can be made to MASAK (RoTF, art. 14(6). Türkiye has a written procedure governing this eventuality. MASAK has also published a guidance in this regard (Guidance on False Positive Cases).

g) MASAK uses an e-notification system to communicate with relevant parties, including most FIs, for instant notification (Law 5549, art. 9/A). In addition to the publishing of the Official Gazette, MASAK is required to expeditiously inform those who have previously indicated that they were holding assets that the decision has been lifted (RoTF, art. 14(4). Furthermore, the cumulative lists of the designees are published in MASAK's web site (https://masak.hmb.gov.tr/bkk-ile-malvarliklari-dondurulanlar). There is a specific guidance to FIs and other persons or entities, including DNFBPs that may by holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action. MASAK has also provided relevant Guidance for applications against freezing decisions regarding the procedure of the 1988 Committee and clear information on how the review of the Committee takes place. The procedure facilitates the review be the Committee. The guidance has been published on the Ministry of Treasury and Finance´s webpage, https://en.hmb.gov.tr/fcib-guidelines.

De-listing, unfreezing and providing access to frozen funds or other assets

Criterion 6.7

Türkiye authorises access to frozen funds or other assets that have been determined to be necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses(Law 6415, arts. 13(2) – (7). While authorising access to assets frozen pursuant to UNSCRs 1267 and 1373, MASAK is required to follow the procedures set out in UNSCR 1452 (2002) and successor resolutions (General Communique No. 12, section 3.1).

> ***Weighting and conclusion –*** Türkiye has mechanisms for implementing TFS related to TF. Even though Türkiye does not consistently implement TF TFS pursuant to UNSCR 1267 without delay, authorities applied other measures to mitigate potential risk and largely bridge the implementation gap when needed. In addition, Türkiye can cancel a freezing request from a foreign country if the requesting country does not initiate an investigation within one year from publication in the Official Gazette. There is no prohibition from making other related services (to financial services) available to designated persons. There are no clear procedures to facilitate review by the 1988 Committee, in accordance with any applicable guidelines or procedures adopted by the 1988 Committee, including those of the Focal Point mechanism established under UNSCR 1730. Recommendation 6 is rated **largely compliant**.

Recommendation 7 – Targeted financial sanctions related to proliferation[57]

In its 2019 MER, Türkiye was rated non-compliant with R.7 and re-rated largely compliant in its 2021 FUR.

Criterion 7.1

TFS related to the financing of the proliferation of mass destruction weapons are set out under Law 7262, also referred to as the "PF Law", adopted in 2020. Law 7262 provides for a legal basis on the application of TFS on UNSC resolutions "on the sanctions for countering the financing of the proliferation of mass destruction weapons" without a reference to specific UNSCRs. The principles and procedures for the implementation of the law are clarified in a regulation (Law 7262, art. 6). In addition, the implementation of TFS within the scope of this law are taken by Presidential Decree and shall be executed without delay upon their publication in the Official Gazette (Law 7262, art. 3).

The Regulation (referred to as "RoPF") regulating the principles and procedures of Law 7262 (RoPF, art. 1) identifies UNSCR 1718 (2006) and successive resolutions and UNSCR 2231 (2015) and successive resolutions as the two regimes for the implementation of PF related TFS (RoPF, art. 3 & 4).

Türkiye adopted three Presidential Decrees (3578, 5967, 10438) to implement PF related TFS. All three Decrees are laying out that the asset freezing decision against persons and entities listed in the annexes, are implemented on the basis of UNSCR 1718 and successive resolutions and UNSCR 2231.

Since 27 September 2025 when the "Snapback Mechanism" to UNSCR 2231 was triggered[58], UNSCR 2231 does no longer contain PF related TFS. PF related TFS on Iran are part of UNSCR 1737 and successors. Following the snapback mechanism, until at the end of the onsite Türkiye had not amended its Presidential Decrees nor the RoPF to include a reference to UNSCR 1737 and successors to ensure the clarity in implementation of UNSCR 1737.

Türkiye is implementing PF related TFS on DPRK in line with UNSCR 1718 (2006) and successive resolutions. The process for the implementation of PF TFS is somehow similar to the one described under criterion 6.4 for TFS implemented as part of UNSCR 1267 and successor resolutions. MASAK is notified without delay of any update of the list, both directly via email and via the Ministry of Foreign Affairs. MASAK then transmits the information to the Presidency of the Republic of Türkiye without delay (RoPF, art. 4). PF TFS gain legal validity once the decision has been taken by the President of the Republic of Türkiye and are to be executed without delay their publication in the Official Gazette (Law 7262, art. 3(1)). This process can occur without delay however as there is no requirement for the decision by the President to be made without delay, TFS are not consistently implemented without delay. However, the mitigating measure described under criterion 6.4 does not apply in the context of PF TFS since the alternative mechanism for the Minister of Treasury and Finance to postpone transactions laid out in Law 5549, art. 19/A applies for ML/TF related transactions.

Criterion 7.2

Designations relevant to proliferation financing and the obligations of FIs and DNFBPs operate similarly to the regime for targeted financial sanctions related to terrorist financing.

a) Türkiye requires that freezing decisions are implemented without delay upon their publication in the Official Gazette (Law 7262, art. 3). All natural and legal persons who keep asset records or hold assets of those for whom asset freezing decision was taken shall take necessary actions to freeze

[57] Recommendation 7 is newly assessed due to changes (implementation) changes that were not assessed during Türkiye's mutual evaluation and follow-up report.

[58] The FATF updated its Standards and Methodology accordingly in October 2025 to refer to the appropriate Security Council resolutions, see https://www.fatf-gafi.org , FATF Update on the re-application of UNSCRs elated to Iran.

the asset without delay (RoPF, art. 11.3). There is nothing in the mechanism which requires prior notice. However, deficiencies in c.7.1 on the absent of explicit provision on UNSCR 1737 and successors also apply to this criterion.

b) The freezing obligation extends to all requirements under this criterion (Law 7262, art. 2 & 3 and RoPF, art. 3).

c) Any funds or other assets are prevented from being made available to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified (Law. 7262, art. 2(1) and RoPF, art. 12).

d) Designations are communicated via the Official Gazette. The decisions shall be immediately notified by to the institutions and organizations (RoPF, art. 8(1). Türkiye provides clear guidance to FIs and other persons or entities, including DNFBPs that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

e) Türkiye requires natural and legal persons who keep asset records or hold assets of those for whom asset freezing decision have been made to take necessary actions to inform MASAK within seven days (RoPF, art. 11).

f) The rights of *bona fide* third parties acting in good faith are protected (RoPF, art 10).

Criterion 7.3

Türkiye has taken measures to facilitate monitoring and ensure compliance by obliged entities with the relevant laws and enforceable means governing the obligations under Recommendation 7. Agencies and ministries which are the members of the Commission on Supervision and Co-operation, monitor for compliance and if required sanction FIs and DNFBPs (RoPF, art 16 & 17). Natural and legal persons identified to be infringing these requirements are to be sanctioned accordingly (Law 7262, art. 5).

Criterion 7.4

a) Türkiye enables listed persons and entities to petition a request for de-listing at the Focal Point for de-listing established pursuant to UNSCR 1730. MASAK has published guidance for applications against freezing decisions which informs persons, entities and organizations whose assets are frozen pursuant to UNSCR 1730 (2006) that they can apply to Focal Points established under the resolution, directly by means of contact information given in the document or through MASAK. The guidance has been published on the Ministry of Treasury and Finance´s webpage, https://ms.hmb.gov.tr/uploads/sites/2/2021/01/Annex_2_A.docx

b) Türkiye has procedures to unfreeze the funds or other assets of persons or entities due to name similarity, false or missing identity information and similar grounds, in such cases the request should be submitted to MASAK in charge of examining the request (RoPF, art. 11(6)). In addition, MASAK has provided Guidance on false positive cases, which explains the procedure to unfreeze funds under the relevant circumstance. The document was published on the MASAK´s website and online meetings were held where the CPF law, guidelines and draft regulations were discussed.

c) Türkiye does authorise the access to funds or other assets, where countries have determined that the exemption conditions set out in UNSCRs 1718 are met, in accordance with the procedures set out in those resolutions (Law 7262, art. 3(6)). This is not the case for UNSCR 1737.

d) The mechanisms for communicating de-listings and unfreezing to the financial sector and the DNFBPs immediately upon taking such action is the Official Gazette. MASAK has provided FIs and other persons or entities, including DNFBPs that may be holding targeted funds or other assets, guidance on their obligations in taking action under freezing mechanisms. The guidance document for the freezing/unfreezing of assets has been published on the MASAK´s website and online meetings were held where the CPF law, guidelines and draft regulations were discussed.

Criterion 7.5

a) All benefits and values derived from funds subject to freezing under UNSCR 1718 are to be frozen (RoPF, art. 3). UNSCR 1737 is not covered in the scope of the RoPF (see criterion 7.1).

b) Türkiye does not prevent designated persons or entities from making any payment due under a contract entered into prior to their listing (RoPF, art. 12 (ç)). However, UNSCR 1737 is not covered in the scope of the RoPF (see criterion 7.1).

> ***Weighting and conclusion –*** Türkiye's framework does not allow for the consistent implementation PF related TFS without delay. UNSCR 1737 and successors resolutions are not covered in the scope of the RoPF and Presidential Decrees, limiting Türkiye's ability to implement PF related TFS on Iran, which has a cascading effect on other criteria. Recommendation 7 is rated **partially compliant**.

Recommendation 8 – Non-profit organisations (NPOs)[59]

In its 2019 MER, Türkiye was rated partially compliant with these requirements and was re-rated largely compliant in its 2023 FUR. Türkiye has not yet been assessed against the 2022 Methodology, which includes substantial revisions to Recommendation 8.

Taking a risk-based approach

Criterion 8.1

a) NPOs in Türkiye consist of associations which are defined as "a society formed by unity of at least seven real persons or legal entities for realisation of a common object other than sharing of profit by collecting information and performing studies for such purpose" (Law 4721). As of July 2025, there were 101,237 associations in Türkiye classified in 22 subgroups, out of which Türkiye considered that 80.195 fall within the FATF definition of NPOs.

Türkiye's General Directorate of Relations with Civil Society (GDRCS), under the Ministry of Interior, is the competent authority responsible for monitoring NPOs (PD No. 1, art. 263). The GDRCS maintains the Associations Information System (DERBIS), which categorises organizations into 22 different activity-based subgroups. To determine the NPOs that fall within the FATF definition, the GDRCS conducts an assessment based on the fields of activities of associations in order to identify the subgroups that pose the lowest TF risk among the 22 different groups. Associations in the subgroups accounting for less than 1% of total financial activity are excluded from the FATF definition of NPO due to their relative financial size, whereas those above this threshold have been included. As a result of the aforementioned calculations, 16 subgroups[60] have been considered to fall within the FATF definition of NPO. Türkiye also excluded 6 subgroups from the FATF definition of NPOs, namely associations for 1) Rights and Advocacy Associations, 2) Thought-Based Associations, 3) Associations Supporting Public Institutions and Personnel, 4) Associations for Relatives of Martyrs and Veterans, 5) Youth Associations, 6) Children's Associations.

[59] Recommendation 8 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

[60] Associations for 1) Professional and Solidarity Associations (social) ,2) Sports and Sports-Related Associations (social and cultural) , 3) Associations Engaged in Activities Related to the Provision of Religious Services (religious), 4) Education Research Associations (education), 5) Culture, Arts, and Tourism Associations (cultural), 6) Humanitarian Aid Associations (charitable), 7) Associations for Preserving Social Values (cultural), 8) Associations Engaged in Health Activities (good works), 9) Urban Planning, Development, and Improvement Associations (good works), 10) International Organizations and Co-operation Associations (good works), 11) Environmental, Natural Life, and Animal Protection Associations (good works), 12) Associations for the Disabled (good works), 13) Associations Active in the Fields of Food, Agriculture, and Animal Husbandry (good works), 14) Associations for Solidarity with Turks Abroad (good works), 15) Associations for the Elderly and Children (good works),16) Associations for Individual Education and Social Development (social).

This approach is not fully in line with the FATF definition of NPOs which focus on function (i.e. raising or disbursing funds), some associations have been included in the scope of NPOs on the basis of their financial materiality rather than on the on the types of activity they carry out and vice versa. This approach has been taken by the authorities to exclude associations subgroups with minimal financial activity.

Similarly, foundations, defined as "private legal entities established by allocating property and rights to a specific and continuous purpose under an organized legal structure" (Law 4721, art. 101) have been excluded from the scope of NPOs based on their low TF risks according to the results of the 2023 and 2025 NRA, and since entrance into the sector requires more rigid procedures. This is not in line with the FATF definition of NPO.

b) Türkiye conducts risk analysis of associations in terms of laundering proceeds of crime and the financing of terrorism, which go beyond the requirements of the FATF methodology focusing on TF risks only. As described above, in line with Türkiye's "Risk-Based Audit Methodology in Combating Laundering Proceeds of Crime and Financing of Terrorism," the GDRCS conducts a preliminary "determination of risk" to identify which associations are at low risk based on their relative financial size. Associations which fall into the subgroups below the 1% threshold described in 8.1(a) are considered to be "low risk" and are not subject to further risk assessment. The GDRCS then scores associations belonging to the remaining subgroups according to a set of weighted criteria that are reviewed and periodically updated as information highlight vulnerabilities in the sector. These criteria include a combination of data points relating to their function, size, channels of income, geographical activity area, and date of establishment; humanitarian aid associations operating in conflict zones are considered to be highly vulnerable to abuse. Based on the 2025 monitoring results, Türkiye identified 131 high-risk and 860 medium-risk NPOs out of a total of 80,195 associations that were examined in the risk assessment.

c) Monitoring of associations is carried under the Law on Associations No. 5253 (art. 19), which establishes the legal basis for audits in accordance with the risk assessment results. This legal framework is supplemented with a set of secondary guidance instruments, including the Directive for Auditors of Associations (art. 21(3), 21(4), and 38(b)), which explicitly includes ML and TF within the audit scope and requires that audit programs be aligned with the outcome of risk analysis. The Guide to Audit of Associations (art. 5 & 12) emphasizes the focus on ML and TF for associations in high and medium risk groups, requires that associations are formally notified of audits at least 24 hours in advance (art. 13), and states that no action can be taken that will prevent or disrupt the activities of associations at all stages of the audit (art. 6). The Audit Guidance on Prevention of Laundering Proceeds of Crime and Financing of Terrorism specifically categorizes TF-related audit scenarios based on risk and provides procedures for referrals to MASAK (art. 8).

Based on the above, Türkiye applies to a certain extent a risk-based approach to address the TF risks identified by NPOs. However, the identification of the subset of organisations falling within the FATF definition of NPO is not fully in line with the Methodology. Türkiye also identifies ML risks related to NPOs and performs oversight activities on the basis of both ML and TF risks which go beyond the requirements of the Methodology.

Sustained outreach concerning terrorist financing issues

Criterion 8.2

a) Türkiye has policies to promote accountability, integrity, and public confidence in the administration and management of NPOs. Persons prosecuted and/or convicted for certain crimes, including ML and TF, cannot be assigned in the organ of an association (Law 5253, art. 3). NPOs must submit yearly expense statements to competent authorities and can be audited (Law 5235,

art. 19), and fines are imposed for non-compliance (art. 32). Türkiye also has legal obligations regarding fund raising, fund using and related auditing activities (Law 2860).

b) Türkiye has a legal requirement for the GDRCS to conduct trainings and workshops to NPOs to raise their awareness on TF risks (Regulation on Associations, additional art. 3 and Circular 20213), and has conducted trainings, with several workshops dedicated to high and medium risk NPOs.

c) Türkiye worked with NPOs to develop and refine best practices to address TF risks. GDRCS has a legal mandate to carry out research and build strategies in co-operation with NPOs, relevant institutions, universities and other research institutions (PD No. 1, art. 263(h)). Türkiye developed guidance to raise awareness among NPOs, such as the "Good Practices Guidance for Preventing NPOs from Abuse for Terrorist Financing Purposes" (2021), the "Guidance Towards Donors of NPOs on Preventing Terrorist Financing Abuse" (2021), the "Guideline for Prevention of Abuse of NPOs for TF" (2021) and the "Guide for Non-profit Organisations on Combating Money Laundering and the Financing of Terrorism" (2025). In addition, GDRCS' published on its website the "Guidance on Principles and Procedures" (2022), covering basic principles of current legislative framework and raises awareness of both associations and the donor community.

d) NPOs are compelled to receive funds from abroad through banks (Law 5253, art. 21). Authorities also encourage NPOs to carry out fund movements within the financial system and where the banking sector does not exist, to use known alternative systems and additional controls to protect their funds (Good Practices Guidance for Preventing NPOs from Abuse for Terrorist Financing Purposes, 2021). In trainings for associations, managers of associations are informed of the legal obligation under the Law on Associations No. 5253 to make all kinds of income, collections, expenses and payments exceeding TRY 7 000 through banks and other FIs (Law No. 5253, art. 32(u)).

Focused, proportionate and risk-based oversight or monitoring of NPOs

Criterion 8.3

a) Türkiye has taken steps to promote focused, proportionate and risk-based monitoring of NPOs.

NPOs are not considered as obliged entities under Türkiye law (Audit Guidance on ML/TF, art. 8) and any natural or legal person has the right to establish an NPO without prior authorisation (Law 5253, art. 3), pending fit and proper requirements.

Türkiye has rules framing the monitoring of NPOs. NPOs are audited in accordance with the assessment of their ML/TF risks, based on the results of risk analyses conducted by GDRCS. Monitoring occurs annually for NPOs considered as high-risk and every two years for medium-risk NPOs (Law 5253, art. 19 and Regulation on Associations, add art. 1) while low-risk NPOs are audited at least every three years (Circular 20213). No action can be taken that will prevent or disrupt the activities of NPOs at all stages of the audit (Guide to Audit of Associations, art. 6). NPOs should receive prior notification ahead of an audit and auditors should limit the scope of the audit to their duty fields (Law 5253, art. 19). Audits are based on a list of established criteria laid out in the Audit Guidance for Combating Laundering Proceeds of Crime and Financing of Terrorism. This monitoring includes a report sent to MASAK if there is sufficient ML/TF suspicion.

b) As described above (8.3.a), NPOs are audited in accordance with the assessment of their ML/TF risks, and this monitoring includes a report sent to MASAK if there is sufficient ML/TF suspicion. The monitoring of NPOs on the basis of ML risks goes beyond the requirements of the methodology.

All NPOs are required to submit a yearly financial statement to competent authorities (Law 5253, art. 19). They are also required to report to competent authorities the aid they receive from people, institutions, and organizations abroad before using it, and to receive this aid through banks. Aid

provided abroad is also to be reported beforehand to the local authority (Law 5253, art. 21). All persons and entities collecting aid in Türkiye should obtain prior authorization from competent authorities (Law. 2860, art. 6). Those measures, applying to the whole NPO sector, are not focused, proportionate and risk-based and may impose burdensome impediments on NPOs activities.

Criterion 8.4

a) As described above under criterion 8.3, competent authorities monitor the compliance of NPOs through audits and requirements in terms of financial reporting and required notification for financial operation from/to abroad. Those measures are focused, proportionate and risk-based to some extent.

b) Türkiye has a broad range of sanctions for NPOs and persons acting on their behalf. It has a range of administrative and judicial sanctions it can apply to natural persons representing NPOs and acting in violations of the obligations. Fines range from 2.321 TRY (approx. 50 EUR) to 1.511.157 TRY (approximately 32.375 EUR) and imprisonment sentences from 3 months to 3 years depending on the severity of the offence (Law 5253, art. 32 and Law 2860, art. 29). Authorities can therefore apply proportionate sanctions depending on the severity of the offence, for instance if the NPO did not keep the statutory books, the responsible person shall be subject to a judicial fine or could face imprisonment up to a year (Law 5253, art. 32 (d)). Executives of associations who do not receive foreign aid through banks are subject to an administrative fine of twenty five percent of the money received in this way (Law 5253, art. 32(c)). Associations that do not meet their legal obligations may be dissolved or suspended, upon request of the Public Prosecutor or any other concerned person who is aware of wrongdoing (Law. 4721, art. 89 & 90). Due to the "individual criminal responsibility" principle of Türkiye's legal system, criminal sanctions can only be applied to natural persons representing the NPOs. As legal persons, NPOs can receive an administrative fine from TRY 10 000 (approx. EUR 206) to TRY 50M (approx. EUR 1M) when committing a range of offences, including TF.

Effective information gathering and investigation

Criterion 8.5

a) Competent authorities co-operate, co-ordinate and share relevant information on NPOs. MASAK and the GDRCS have a protocol for the exchange of information, co-operation and co-ordination on NPOs. MASAK is notified of the outcomes of NPOs audits (Audit Guidance on ML/TF). Databases on NPOs (DERBIS) are held by the GDRCS and include information on institutional data, founder and manager information, immovable property, vehicle information, public relief, financial aid and foreign aid. These databases are directly available to MASAK, the Turkish National Police and the Turkish General Command of the Gendarmerie.

b) GDRCS conducts monitoring and audit activities of NPOs and notifies competent authorities when it detects suspicious TF related activity (Audit Guidance on Prevention of ML/TF, art. 8). There are a total of 121 auditors at the GDRCS, including 78 Association Auditors and 43 Association Auditor Assistants. NPOs auditors are required to pass a proficiency exam to ensure that they have the required competencies to perform their duties (Regulation Concerning Auditors of Associations, art. 31). MASAK has the authority to collect data, to receive STR, to analyse and evaluate them in the scope of prevention of ML/TF (PD No.1, art. 231 (c)). Based on its analysis, MASAK may convey cases to the Public Prosecutor's Office when serious suspicion of TF is identifies, including in the case of NPO abuse.

c) MASAK, the Turkish National Police and the Turkish General Command of Gendarmerie have direct access to information on NPOs through the DERBIS database. During audits of NPOs, upon the request of the assigned officers, any information, document, and record must be presented and

full access to the premises must be provided (Law No. 5253, art. 19). Moreover, public prosecutors and LEAs working under the command of the prosecutors are authorized to access relevant information related to administration and management of NPOs, in the course of an investigation (Criminal Procedure Law, art.161). In addition, a civil servant who detects situations that give rise to serious suspicions is obliged to report the suspected offence to the competent public institutions and organisations, by virtue of his or her responsibilities as a civil servant (Turkish Criminal Law, art. 279).

d) Türkiye has established mechanisms to deal with cases when there is a suspicion or reasonable grounds to suspect that a particular NPO is involved in TF related activities. If any offense is detected during an audit, the GDRCS immediately notifies the Public Prosecutor's Office and the association (Law. 5253, art. 19). If, while exercising its duties, MASAK identifies serious suspicion that a TF offence has been committed by, or through, an NPO, the case is conveyed to the Public Prosecutor's Office (PD No. 1, arts. 231(e)) and if analyses conducted by MASAK reveal some suspicions, the case can be conveyed to the Chief Public Prosecutor's Office for further investigation (PD No. 1, arts. 231 (f)).

Effective capacity to respond to international requests for information about an NPO of concern

Criterion 8.6

MASAK is the central point of contact for information sharing with foreign counterparts regarding any NPO suspected of terrorist financing or involvement in other forms of terrorist support. MASAK has authority to exchange information and documents with counterparts in foreign countries, and for this purpose, to sign memorandum of understanding (PD No.1, art. 231 (1)(l) and (5)). Moreover, exchange of information request may be received through formal channels or in the course of police co-operation. Ministry of Justice serves as the central authority in terms of responding mutual legal assistance requests (Law no 6706, art.2[1][b]). In terms of police co-operation, the exchange of information may be ensured through liaison officers or through Interpol-Europol Department (TNP Internal Circular No 2009/36).

> ***Weighting and conclusion –*** Türkiye is monitoring the compliance of at risk NPOs with focused, proportionate and risk-based measures to a certain extent. The legal framework allows for a wide range of measures, applying to the whole NPO sector, which are not specifically designed based on TF risks and can impose some burdensome impediments on NPOs activities that could lead to disrupt the legitimate activities of the sector. NPOs can also be monitored for ML and not only in relation to TF. The identification of the subset of organisations falling within the NPO category is not fully consistent with the FATF functional definition, yet this deficiency has been weighted less heavily in Türkiye's context as it did not prevent authorities from conducting a robust risk assessment of the NPO sector. Authorities have engaged with the sector to a large extent in awareness activities and demonstrated efforts to monitor the sector without disrupting legitimate activities, despite this broad framework (see IO.10). Recommendation 8 is rated **partially compliant**.

Recommendation 9 – Financial institution secrecy laws[61]

In its 2019 MER, Türkiye was rated compliant with R.9.

[61] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019 with non-substantive edits from Türkiye.

Criterion 9.1

There are no financial institution secrecy laws that inhibit the implementation of the FATF Recommendations.

a) Access to and sharing of information between competent authorities: MASAK has powers to require necessary information and documents: Law No. 5549, art. 7; and ROM, arts. 31 and 36. Failure to comply results in imprisonment (up to three years) and a judicial fine (up to 5 000 days, which is the equivalent of TRY 2 500 000 or EUR 68 530): art. 14 and 7 of Law No. 5549. In addition, examiners appointed by MASAK have the power to obtain information and documents upon request, including through examination: Presidential Decree No. 1, arts. 231(4); Law No. 5549, art. 7 and 11; and RoM art. 36(2). Failure to provide inspectors with information is subject to same penalties, as those set out above. Institutions receiving a request for information are subject to a non-self-incrimination provision. MASAK can share information it possesses with other authorities.

   The BRSA has powers to obtain information: Law No. 5411, arts. 38, 95 and 96. Penalties of imprisonment for one to three years and a judicial fines of 500 to 1 500 days is available for non-compliance; Law No. 5411 art. 153. BRSA also has powers to obtain information in relation to financial leasing as well as factoring and financing companies: Law No. 6361, art. 17. Prison sentences and administrative fines are available for non-compliance: Law No. 6361, art. 47. In relation to the card payments system, BRSA has powers to require information and both administrative fines and prison sentences are available for non-compliance: Law No. 5464, art. 27. With regard to payment services and electronic money institutions, there are powers for the CBRT to obtain information: Law No. 6493, arts. 8 and 21. Prison sentences and fines are applicable in relation to non-compliance. CBRT and BRSA can share information with MASAK, public prosecutors and criminal courts as well as its foreign counterparts.

   The CMB also has power to obtain information: CML, arts. 89 and 90. A person failing to provide information is subject to imprisonment: CML, art. 111. The CMB is able to provide information to other authorities voluntarily (without receiving a request) for financial stability purposes and meet other domestic and international requirements: CML, art. 128.

   The IPRSA can obtain information from insurers and intermediaries: Law No. 5684, arts. 28 and 29. Penalties for non-compliance include imprisonment and fines. With regard to pension companies, the IPRSA can obtain information: Law No. 4632, arts. 11(f) and 20. Penalties for non-compliance include imprisonment and fines.

   The MoTF may require information from exchange offices under Treasury Communique No. 2018-32/45, arts. 19 and 28. The legal framework mentioned above also provides provisions to overcome confidentiality to which the person requested to provide information is subject. MoTF can share information with domestic and foreign competent authorities. See c.31.4 for the powers of law enforcement authorities to obtain information.

b) Sharing of information between financial institutions: There are no provisions preventing the exchange of information by FIs for the purposes of compliance with Recommendations 13, 16 and 17. See those Recommendations for compliance with these specific criteria.

Weighting and conclusion – The criterion is met. Recommendation 9 is rated **compliant**.

Recommendation 10 – Customer due diligence[62]

In its 2019 MER, Türkiye was rated largely compliant with R.10. There were minor shortcomings related to the lack of explicit reference to parties to a legal arrangement and requirement not to open an account or terminate the business relationship applying only in case of suspicion relating to customer identification, rather than all relevant CDD measures.

Criterion 10.1

FIs are prohibited from opening anonymous accounts or accounts in fictitious names: RoM, art. 22(1). Banks are obliged to not open deposit, investment fund, credit or other accounts or provide remittance and foreign exchange services to clients who do not document their identities and tax numbers: Law 5411, art.76, and intermediaries cannot open fictitious accounts: CMB Communique III-39.1, art.56(h).

When CDD is required

Criterion 10.2

FIs are required to undertake CDD when:

a) establishing business relations: RoM, art.5(1)(a);

   carrying out occasional transactions above the designated threshold TRY 185 000 (EUR 5 071) / 15 000 (EUR 411) for CASPs including situations where the transaction is carried out in a single operation or in several operations that appear to be linked : RoM, art.5(1)(b);

b) carrying out occasional transactions that are wire transfers above the designated threshold TRY 15 000 (EUR 411) : RoM, art.5(1) (c);

c) regardless of any exemptions or threshold, in cases of suspicions of ML/TF : ROM, art.5(1)(d);

d) In cases where there is doubt about the adequacy and the accuracy of previously obtained customer identification information: ROM, art. 5(1)(e).

Required CDD measures for all customers

Criterion 10.3

FIs are required to identify natural and legal persons carrying out transactions and persons on whose behalf or for whom the transactions are conducted: Law 5549, art.5(1) and RoM, art.14. Chapter 3 of RoM defines principles and procedures regarding CDD obligations for the implementation of Law 5549. It specifies a range of natural and legal persons for whom CDD obligations apply, including unincorporated organisations and remote customer identification for natural persons and legal persons enrolled to the trade registry (RoM, art.6/A). Furthermore, Türkiye is not a party to The Hague Convention and in this regard does not recognise trusts and legal arrangements. However, in case a transaction requiring customer identification is requested from an obliged entity by a natural or legal person trustee of a trust agreement established abroad, the customer identification will be carried out in accordance with article 11(2) of RoM which includes identifying all parties to the trust. Customer identification consists of the receipt of identification information and verification of its accuracy (RoM, art.5). The types of document and/or source of document specified amount to reliable, independent source documents, data or information (RoM, arts.6 to 14).

[62] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019 with minor non-substantial edits from Türkiye.

Criterion 10.4

FIs are required to identify natural and legal persons acting on behalf of the customer (see criterion 10.3). In addition, verification that a person acting on behalf of a customer is so authorised and of that person's identity is required: RoM, art.14.

Criterion 10.5

Beneficial owner (BO) is defined as a natural person(s) who has ultimate control or influence over a natural person(s) who carries out a transaction within an obliged entity, or over the natural persons, legal persons or unincorporated organisations on whose behalf a transaction is being conducted within an obliged entity (RoM, art. 3(h)). FIs must take the necessary measures to identify their customers by receiving their identification information and verifying it and take necessary measures for revealing the beneficial owner (RoM, art. 5) and the identity of BO must be verified (RoM, art.17/A(6)). However, it is unclear what are the relevant information or reliable source that FIs should use.

Türkiye does not recognise trusts and legal arrangements. However, in case a transaction requiring customer identification is requested from an obliged entity by a natural or legal person trustee of a trust agreement established abroad, the customer identification will be carried out (RoM, article. 11(2)). For identification of the beneficial owner, identity information of the settlor, beneficiary or groups of beneficiaries and protectors, if any, shall be received and reasonable measures shall be taken for verifying this information. Necessary measures shall also be taken for revealing the natural person(s) who ultimately control(s) the mentioned assets.

Criterion 10.6

Information on the purpose and intended nature of the business relationship must be obtained before entering into a business relationship or conducting a transaction: RoM, arts. 5(3) and 22. FIs are required to obtain information on the profession of individuals: RoM, art.6, as well as on the business of other customers: RoM, arts.7-14. RoM, art.19 requires monitoring of transactions and whether they are consistent with the business relationship. This and the requirement for on-going monitoring of all customers as to whether the transactions they conduct are consistent with the information regarding business, risk profile and fund resources (art. 15(3)(f) of the RoC) will indirectly require the purpose and intended nature to be understood.

Criterion 10.7

FIs are required to conduct ongoing due diligence on the business relationship:

a) Ongoing monitoring of transactions is required to ascertain whether they conform to the information held on the customer's profession, commercial activities, business history, financial status, risk profile and source of funds: RoM, art.19(1). In addition, FIs listed in art.4 of the ROC are also required to perform monitoring: ROC, art.14. Within the scope of this obligation, they are required to perform controls on customer-related information and documents, including the information contained in wire transfer messages: RoC, art. 15(3)(e), and conduct ongoing monitoring as to whether the transaction conducted by the customer is consistent with the information regarding the customer's business, risk profile and source of funds: RoC, art.15(3)(f). FIs must develop rules for ensuring the monitoring and control of risky customers, transactions and services: RoC, art. 12.
b) There is a requirement to keep up-to-date information, documents and records regarding the customer, as well as verify contact and address details: RoM, art.19. It is implied that information be kept relevant. In the case of higher risk categories of customers identified by FIs, enhanced monitoring must be undertaken: RoM, art.26/A(1)(e) and ROC, art. 13.

Specific CDD measures required for legal persons and legal arrangements

Criterion 10.8

There are general requirements to identify the customer and those who act on behalf of or for the benefit of customers, and gather information on the purpose and intended nature of the business relationship: RoM, arts. 5(1), 5(3). In the case of legal persons registered at the Turkish trade registry, FIs must obtain information on the field of activity: RoM, art.7. For associations, foundations, trade unions, confederations and unincorporated associations, FIs must obtain information on their aims: RoM, arts.8, 9 and 12. Art.11 addresses the identification of non-resident legal persons, requiring information equivalent to that for Turkish legal persons. Also see the provisions on BO under criterion 10.5, above. These, together with ongoing monitoring obligations, may mitigate the gap of lack of an express requirement to understand the customer's ownership and control structure. Türkiye is a non-trust law country, however, in case a transaction requiring customer identification is requested from an obliged entity by a natural or legal person trustee of a trust agreement established abroad, the customer identification will be carried out in accordance with Article 11(2) of RoM and verified through the trust deed. This also includes identification of parties (trustee, settlor, beneficiary, protector) to these arrangements with regards to identification of BO hence its relevant terminology is not explicitly outlined in the domestic legislation. These, together with ongoing monitoring obligations, ensures that financial institutions understand the customer's ownership and control structure.

Criterion 10.9

For legal persons, name, legal form, trade registry number and proof of address is required to be identified and verified through documents of registration to the trade registry. This would include the powers that regulate and bind the legal person and the names of relevant persons holding a senior management position. The trade registry will have registered office address as well as address of principal place of business if different from registered address, if a company uses two addresses. These obligations do not explicitly apply to customers that are legal arrangements, however, FIs also have a general obligation to identify and verify their customers by obtaining their identification information and verifying it.

Criterion 10.10

Beneficial owner (BO) is defined as a natural person(s) who has ultimate control or influence over a natural person(s) who carries out a transaction within an obliged entity, or over the natural persons, legal persons or unincorporated organisations on whose behalf a transaction is being conducted within an obliged entity (RoM, art. 3(h)). FIs must take necessary measures to reveal the beneficial owner i) when establishing a permanent business relationship with legal persons; ii) when the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than TRY 185 000 (approx. EUR 3 800) (TRY 15 000 (approx. EUR 307 for VASPs); iii) or is equal to or more than TRY 15 000 (approx. EUR 307) for wire transfers, VAs transactions or transactions conducted by VASPs; iv) regardless of the monetary amount in cases requiring STR; v) regardless of the monetary amounts in cases where there is suspicion about the adequacy and the accuracy of previously acquired identification information (RoM article. 5(1)).

FIs must:

a) Identify natural person partners holding more than 25% of the legal person's shares as the beneficial owner (RoM, art.17/A(2)).
b) When there is doubt that the natural person partner holding more than twenty-five percent of the legal person's shares is not the beneficial owner or where there is no natural person holding a share at this rate, necessary measures shall be taken in order to identify the natural person(s) who is/are ultimately controlling the legal person. Natural person(s) identified shall be considered as beneficial owner (RoM, art. 17/A(3)).

c) Where no natural person is identified under (a) and (b) above, the natural person(s) holding the position of senior managing official in the trade registry with the highest executive authority, shall be considered as beneficial owner (RoM, art. 17/A(4)).

Criterion 10.11

Türkiye does not recognise trusts and legal arrangements. However, in case a transaction requiring customer identification requested from an obliged entity by a natural or legal person trustee of a trust agreement established abroad, the customer identification will be carried out in accordance with Article 11(2) of RoM. This includes identification of parties (trustee, settlor, beneficiary or group of beneficiaries and protectors, if any) to these arrangements with regards to identification of BO. Additionally, necessary measures also needs to be taken for revealing the natural person(s) who ultimately control(s) the assets of a trust agreement established abroad: ROM, art.11(2).While other types of legal arrangements will be captured by customer identification provisions in RoM, art.12[63] , art. 14[64] and art.17/A(5)[65].

CDD for Beneficiaries of Life Insurance Policies

Criterion 10.12

Sub-criterion (a): Art. 1493(2) of the TCC requires life insurance policy holders to disclose the beneficiary of insurance policies to insurance companies; this includes beneficiary's name. Specific provisions are not included for sub-criteria (b) and (c) but the gap is reduced as FIs are required to detect whether a transaction is being carried out for the benefit of another person: ROM, art.17(1). Where a person declares that (s)he is acting for the benefit of someone else, the benefitting person must be identified; although, it is not clear if verification is also covered by this. Where there is a suspicion that a person acting in his own name is in fact acting for the benefit of another person, measures for the identification of BO must be applied. In addition, in its FAQs, MASAK states that "the insured or the beneficiary will also be identified while carrying out a transaction (such as payment) requiring identification of these persons." This does not cover verification of beneficiary's identity.

Criterion 10.13

There are no specific provisions that require FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. This is somewhat mitigated by the general requirement to take customer risk factors into account in deciding whether to apply enhanced CDD and the sectoral STR guideline for FIs, to regard life insurance policies as risky where a customer applies for life insurance not compatible with the customer's age and health status or accepts such conditions without question.

Timing of verification

Criterion 10.14

Delayed verification is not permitted: art. 5(1) RoM.

Criterion 10.15

Delayed verification is not permitted: art. 5(1) RoM.

[63] ROM, art. 12 addresses unincorporated organisations and organisations, such as unincorporated joint ventures.

[64] ROM, art. 14 addresses customer identification of those acting on behalf of others.

[65] ROM, art. 17(A)/5 addresses unincorporated organisations and the need to detect the natural person ultimately controlling "the legal person" and, where no such person is detected, the senior managing official are considered to be the beneficial owner.

Existing customers

Criterion 10.16

Provisional Art. 2 of ROM requires FIs to apply CDD requirements to the existing customers as on 1st September 2008. In this scope they were required to adjust existing customers' identification information to ROM by 1st September 2009: MASAK Communiqué No.8. If an FI cannot conduct customer identification, it shall not establish a business relationship and not conduct the transaction: art. 22(1). In cases where customer identification cannot be carried out due to suspicion on the adequacy and accuracy of the previously obtained customer identification information, the business relationship will be terminated: art. 22(1). Within the scope of permanent business relationships obliged entities are required to continuously follow up whether the transactions conducted by their customers are in compliance with the information regarding the customer's profession, commercial activities, business history, financial status, risk profile and sources of funds and keep up-to-date information, documents and records regarding the customer. Additionally, financial institutions also have to take necessary measures in order to follow up the transactions conducted out of permanent business relationship in risk-based approach: RoM, art. 19(1).

Risk-Based Approach

Criterion 10.17

FIs must apply one or more of a series of defined enhanced measures, in proportion to the identified risk, for higher-risk situations that they identify in the framework of a RBA: ROM, art.26/A. The application of such measures is also required for transactions within the scope of art.18 (special attention – complex and unusual large transactions and transactions which have no apparent legitimate and economic purpose), art.20 (measures against technological risks) and art.25 (relationships with risky countries). In addition, the MoTF may separately determine whether a country represents a high-risk situation to be taken into account within the scope of art.26/A. MoTF may also determine enhanced measures different to those specified in the article. No such determinations have been made. Art. 13 of the ROC contains identical provisions on enhanced measures.

Criterion 10.18

MoTF allows FIs to take simplified measures for self-transactions; where the customer is a public administration or quasi-public professional organisation; in establishing a business relationship within the scope of salary payment by accepting a batch of customers; in transactions related to pension schemes that provide retirement benefits through deduction from salaries and of pension agreements; in transactions where the customer is a public company with its shares listed on the Turkish stock exchange: ROM, art.26. Further, MASAK Communiqué 5 clarifies the applicable measures and transaction types covered under the article. Further, in each case where simplified measures may be applied, FIs shall assess each transaction separately whether there will be any abuse of transaction for ML/TF and, therefore, whether there is any ML/TF risk. In the event that there is a suspicion of ML/TF, FIs shall not apply simplified measures and shall report the transaction to MASAK as an STR: art. 2(1), MASAK Communiqué 5.

Failure to satisfactorily complete CDD

Criterion 10.19

a) When FIs cannot identify the customer and the BO (RoM, art. 5(1)), or obtain information on the purpose of the business relationship, they are required not to open the account, commence business relations or perform the transaction: RoM, art. 22(1). Where customer identification and verification cannot be conducted due to suspicion on the adequacy and accuracy of previously obtained customer identification information, FIs are required to terminate the business

relationship: RoM, art.22(2). There is a gap in that the provisions of art.22 do not apply to all relevant CDD measures and relate only to customer identification.

b) FIs are required to consider whether the situations falling under art. 22(1), as described above and art 22(2), are suspicious (meaning in practice that consideration must be given to filing an STR): RoM, art.22(3). The gap therefore described in c.10.19(a) largely applies here; although, it is further reduced, by the examples in the STR Guideline on STR Filing when CDD cannot be completed satisfactorily.

CDD and tipping-off

Criterion 10.20

When FIs cannot identify the customer and the BO (RoM, art. 5(1)), or obtain information on the purpose of the business relationship, they are required not to open the account, commence business relations or perform the transaction: RoM, art. 22(1). Where customer identification and verification cannot be conducted due to suspicion on the adequacy and accuracy of previously obtained customer identification information, FIs are required to terminate the business relationship: RoM, art.22(2). There is a gap in that the provisions of art.22 do not apply to all relevant CDD measures and relate only to customer identification.

FIs are required to consider whether the situations falling under art. 22(1), as described above and art 22(2), are suspicious (meaning in practice that consideration must be given to filing an STR): RoM, art.22(3). The gap therefore described in c.10.19(a) largely applies here; although, it is further reduced, by the examples in the STR Guideline on STR Filing when CDD cannot be completed satisfactorily.

> ***Weighting and conclusion –*** Türkiye meets the core CDD requirements such as identification and verification of customer and beneficial owner. There are minor deficiencies related to lack of requirements to consider beneficiaries as a risk factor and requirement to not to open account or terminate business relationship applying only in case of suspicion relating to customer identification, rather than all relevant CDD measures. Recommendation 10 is rated **largely compliant**.

Recommendation 11 – Record-keeping[66]

In its 2019 MER, Türkiye was rated compliant with R.11.

Criterion 11.1

FIs are required to maintain records on transactions, both domestic and international, for at least eight years following completion of the transaction: Law 5549, art. 8 and RoM art. 46.

Criterion 11.2

FIs are required to retain the documents, books and records, identification documents and records kept in all forms regarding their transactions and obligations, for eight years. The obligation is triggered from the date of issue of documents, from the last date on which the last record was made for books and records, and from the date on which the last transaction was made for identification documents. These provisions cover the termination of the business relationship and the date of the occasional transaction. Documents and records of suspicious transactions reports made to MASAK or internal reports made to the compliance officer, documents attached to reports, the written reasons relating to suspicious transactions decided not to be reported by compliance officers are all in the scope of obligation of retaining and submitting (RoM, art.46(2)). Records in all forms seem to implicitly cover account files and business correspondence. In

[66] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019.

addition, TCC (art. 64 and 82) requires all commercial letters received and copies of commercial letters sent to be retained by every trader for ten years.

Criterion 11.3

There is no specific language relating to reconstruction of individual transactions to provide, if necessary, evidence for prosecution of criminal activity. However, art. 217 of the Criminal Code, which allows all kinds of legally obtained evidence to be used as evidence; and the totality of the detailed requirements on CDD, transactions, the legal provisions enabling the authorities to obtain information and the provisions articulated above for criterion 11.1 and 11.2 provide necessary available evidence for inquiries into criminal acts. There is no language limiting the keeping of transaction records.

Criterion 11.4

FIs are required to ensure that all information, including CDD information and transaction records, are available to MASAK upon appropriate authority: art.7 of Law No. 5549 and ROM, art. 31. The requirement to provide information must be made in writing, except in urgent situations. In cases where information is required in writing it must be submitted within a period of no less than seven days (the seven day requirement is to protect FIs taking into account formal procedural duration, information is provided earlier if available). When information is required verbally (i.e. in urgent situations), any deadline for the provision of information can be imposed as there is no limiting factor in the legislation; such verbal communications must be followed up in written form. Responses to verbal communications are made within the required timeframes and do not trigger the seven-day requirements.

> *Weighting and conclusion –* All criteria are met. Recommendation 11 is rated **compliant.**

Recommendation 12 – Politically exposed persons (PEPs) [67]

In its 2019 MER, Türkiye was rated non-compliant with R.12 and re-rated compliant in its 2023 FUR.

Criterion 12.1

Türkiye introduced specific references to foreign PEPs in its AML/CFT legislation, MASAK General Communique No. 21 on PEPs (Com. 21) that entered into force on 17 November 2022 (issued pursuant to ROM [68], art. 26/A and ROC [69], art. 13). Art. 3(1)d of the Com. defines PEPs [70] , with a set of categories of senior natural persons widely enough to cover the FATF definition. In addition to performing the CDD measures under R.10, FIs are required to carry out the following in respect of foreign PEPs:

a) Include in the risk management systems measures to determine whether a customer or the beneficial owner is a foreign PEP (Com. 21, art.4(2) and art.4(1));
b) obtain senior management approval before establishing (or continuing, for existing customers) such business relationships (Com. 21, art.4(3)a and art.4(1));
c) take reasonable measures to establish the source of the assets and funds that belong to customers and beneficial owners identified as PEPs or that are the subject of the transaction (Com. 21, art.4(3)b and art.4(1));
d) conduct enhanced ongoing monitoring on that relationship (Com. 21, art.4(3)c and art.4(1)).

[67] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019 and FUR 2023.

[68] Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism.

[69] Regulation on Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism.

[70] Politically exposed person means senior natural persons entrusted with prominent public functions domestically or in a foreign country by election or appointment, and members of the executive board and senior management of international organizations and individuals entrusted with equivalent functions in such organizations.

Criterion 12.2

The definition of PEPs covers in addition to domestic PEPs, persons who have been entrusted with a prominent function by an international organisation (Com.21, art. 3 (1)(d)). In relation to these persons, FIs are required to:

a) Take reasonable measures to determine whether the Customer or the Beneficial Owner is considered one of those persons (Com.21, art.4(1)).

b) Take the measures identified in relation to clauses b) to d) under Criterion 12.1 above, when there is a high-risk business relationship accompanying such persons (Com.21, art.4(4)).

Criterion 12.3

FIs are required to apply the enhanced measures set out in c.12.1 to spouses, first degree relatives or close associates of foreign PEPs (Com.21, art.4(3)); and to spouses, first degree relatives or close associates of domestic PEPs and persons who have been entrusted with a prominent function by an international organisation when domestic PEPs and persons who have been entrusted with a prominent function by an international organisation are considered to pose high risk in line with c.12.2 (Com.21, art.4(4)). 'Close associates' refers to any kind of social, cultural or economic relation, such as being relative other than by first degree, being a fiancé, being a company partner or employee, which can be considered an association of interest or purpose. (Com.21, 4(6)).

Criterion 12.4

In relation to life insurance policies, FIs are required to take reasonable measures before or at the latest at the time of the payment of insurance policy-related rights and claims to the beneficiary to determine whether the beneficiaries or beneficial owners of a life insurance policy are PEPs (Com.21, art.4(5)). If a high risk has been identified, senior management shall be informed before making the payment and enhanced scrutiny as set out in c.12.1 (d) must be applied (Com.21, art4(5). There is no specific requirement in the Com. to consider making an STR when higher risks are identified but the general requirement to report suspicious activity (based on art.4 of AML Law and art.27 of the RoM) applies. In addition, the PEP Guidance requires obliged entities to inform MASAK when higher risks are identified regardless of whether the PEP is a domestic, foreign or international organization PEP.

Weighting and conclusion – All criteria are met. Recommendation 12 is rated **compliant**.

Recommendation 13 – Correspondent banking[71]

In its 2019 MER, Türkiye was rated largely compliant with R.13 because of a minor gap regarding understanding fully the nature of the respondent's business which has now been addressed.

Criterion 13.1

In relation to cross-border correspondent banking and other similar relationships, FIs are required to do the following (ROM, art.23.1):

a) obtain, by making use of publicly available resources, reliable information on whether the respondent FI has been subject to a ML/TF investigation or been sanctioned or warned; its business nature and field; reputation; and the adequacy of its supervision. Through the amendments made to article 23.1 of RoM in 2021, obtaining the nature of the business related to respondent parties is incorporated into the RoM.

[71] Recommendation 13 is assessed considering legislative and regulatory changes in Türkiye.

b) assess the respondent institution's AML/CFT controls;
c) obtain approval from senior management before establishing new correspondent relationships; and
d) clearly understand the respective AML/CFT responsibilities of each institution.

Criterion 13.2

With respect to "payable-through accounts," FIs are required to satisfy themselves that the respondent bank:

a) has performed CDD obligations on its customers that have direct access to the accounts of the correspondent bank: ROM, art. 23(d).; and
b) is able to provide relevant CDD information upon request to the correspondent bank: ROM, art. 23(d).

Criterion 13.3

FIs are prohibited from entering into or continuing correspondent relationships with shell banks, as well as banking relationships with banks where there is doubt as to whether or not the bank permits their accounts to be used by shell banks: ROM, art. 23(2).

> *Weighting and conclusion –* All criteria are met. Recommendation 13 is rated **compliant.**

Recommendation 14 – Money or value transfer services[72]

In its 2019 MER, Türkiye was rated largely compliant with R.14 because of the lack of a mechanism or unit specifically focused on identifying unlicensed or unregistered providers which has been established since.

Criterion 14.1

Money or value transfer services are described as a "payment service:" Law 6493, art. 12.1. Natural or legal persons intending to operate in the field of payment services must first obtain permission from the Central Bank of the Republic of Türkiye (CBRT), in accordance with applicable conditions: Law No. 6493, art. 14.1 and 14.2.

Criterion 14.2

The supervision of payment systems is performed by CBRT. The CBRT is also entitled to supervise the branches and agents of payment institutions or the entities to which activities are outsourced by these institutions: Law 6493, arts. 21.1 and 21.2. The investigation and prosecution of unlicensed individuals and entities is subject to written request by CBRT to the Chief Public Prosecutor's Office: Law No. 6493, art. 37.1. The CBRT established the Payment Systems and Financial Technologies Department within CBRT Head Office to, among others, focus on unlicensed or unregistered providers and working on complaints regarding illegal MVTS activities. The CRBT also published guidance explaining the public how to identify illegal services providers.

CBRT relies on denunciations, which may be made to them on an ad hoc basis by outside parties, including law enforcement and financial institutions. CBRT may also become aware of unlicensed MVTS providers in the course of an examination. On sanctions, real persons and officers of legal persons who act as a payment institution without the required licensing and registration are subject to imprisonment for one to three years and a judicial fine of up to 5 000 days (up to 5 000 days, which is equivalent to a maximum amount of TRY 2 500 000 or EUR 68 530): Law No. 6493, art. 28.1 and 28.2.

[72] Recommendation 14 is assessed considering legislative and regulatory changes in Türkiye.

Table A.1. Number of Denunciations by CBRT to the Public Prosecutor (2020 - 2024)

Crime	2020	2021	2022	2023	2024
Operating without license (Violation of Article 28 of the Law No.6493)	51	175	139	334	299*

Note: *Data as of :13.10.2024.*

Criterion 14.3

MVTS providers, as licensed payment institutions, are subject to AML/CFT obligations, including monitoring for AML/CFT compliance: RoM, art. 4.1, Law No. 5549, art. 11 and RoM, Chapter 6. MASAK is designated as the supervisory authority: Presidential Decree No. 1, art. 231.1(i). MASAK, as the supervisory body, has the authority to ensure supervision of obligations within the scope of AML/CFT: Presidential Decree No.1, art. 231(1)(i). In the normal course of business, CBRT conducts examinations of MVTS providers, but these examinations are focused on prudential concerns. However, CBRT examiners are required to immediately report AML/CFT violations discovered in the course of this work to MASAK in writing: RoM, art. 40(1). MASAK may also request for examiners to inspect relevant MVTS providers on a case-by-case basis or under the scope of a supervisory program: RoM, art. 35(2).

Criterion 14.4

Payment institutions are required to maintain a current list of their agents and make the list publicly accessible on their website: ROPS, art. 18.6.

Criterion 14.5

Payment institutions are required to set up internal control methods for the purposes of fulfilling AML/CFT obligations and preventing fraud: ROPS, art. 18.19. Payment institutions are also required to monitor their agents via a centralised system: ROPS, art. 18.15.

Weighting and conclusion – All criteria are met. Recommendation 14 is rated **compliant.**

Recommendation 15 – New technologies[73]

Türkiye was largely compliant in its 2019 MER (former R.15), re-rated non-compliant in its 2021 FUR and partially compliant in its 2023 FUR primarily because VASP were not required to be registered or licensed at the time

New technologies

Criterion 15.1

In its 2023 FUR, Türkiye met the requirement of this criterion. MASAK is authorised to conduct risk assessment studies at national level with institutions and organisations in order to combat ML and TF (PD No. 1, art. 231/1(a)). In addition, FIs should identify ML/TF risks of new products and new business applications/practices and the use of new and developing technologies (RoM, art.20). This art. should be read in conjunction with RoC (art.11 and 12) where FIs are required to develop a risk management policy with the aim of defining […], assessing and reducing the risk and where risk management activities cover rating and classifying services, transactions and customers depending on risks and in particular with art.

[73] Recommendation 15 is assessed considering legislative and regulatory changes in Türkiye.

15(3)(g) RoC, where monitoring and control activities should include risk-based control of services that may become prone to misuse due to newly introduced products and technological developments.

Criterion 15.2

In its 2023 FUR, Türkiye met the requirement of this criterion. FIs are required to "pay special attention to" the risks of ML/TF posed by new and developing technologies, existing and new products (including new delivery channels) and new business applications and to "take appropriate measures for its prevention" (RoM, art.20(1)). Pursuant to RoM art.20(2), they are required to: (i) pay special attention to operations such as establishment of permanent business relationships, depositing, withdrawing and wire transfers which are carried out through non face-to-face transactions; (ii) closely monitor the transactions which are not consistent with the risk profile of the customer or do not have relation with his/her activities; and (iii) establish a limit to amount and number of transactions. FIs are also required to apply enhanced measures for high-risk situations (RoM, art. 26/A).

Virtual assets and virtual asset providers

Criterion 15.3

In accordance with Recommendation 1:

a) MASAK conducted in 2022 a strategic analysis to determine the ML/TF risks of virtual assets (VAs) and virtual assets service providers (VASPs) in Türkiye. This analysis was updated in 2025, considering developments in the sector. The analysis is comprised of 15 risk criteria (size of the sector, diversity of products and services, results of supervisions, etc). The sector is considered as posing a high risk for ML/TF mainly due to its size, diversity of products, high number of VASPs in violation of their ML/TF obligations, high number of violations determined in the supervisions, high number of STRs. Türkiye also identified and assessed PF risks emerging from VAs activities and VASPs in the context of its 2025 PF NRA. MASAK conducted this analysis, taking into account 20 risk factors. It was assessed that the PF risk level of the sector is medium mainly due to the fact that it is a newly licensed and supervised sector, it poses a high ML/TF risk and VAs can be abused in connection with PF activities in global PF typologies. The activities of the VASPs in the analysis are in line with the definition of VASPs in FATF Glossary.

b)

   i. Since 2024, VASPs are considered as financial institutions in Türkiye (RoM, art. 3(1)(f)). As financial institutions, VASPs are subject to the general preventive measures (CDD, identification of beneficial owner, suspicious transaction reporting) and enhanced measures in high-risk situations (RoM art. 26/A). VASPs are also required to prepare risk-based compliance programmes (RoC, art. 4(1)(ı)) and appoint a compliance officer to conduct this program (RoC, art. 16(1)). When other FIs are establishing business relationships with VASPs and when VASPs are establishing business relationships with their customers, they are required to take additional measures such as information on the source of the assets subject to the transaction and source of funds of the customer; reasons for the transaction; enhanced monitoring (RoC, art.13(2)).

   ii. As an obliged entity, VASPs should develop institutional policies related to risk management, monitoring and control, training and internal audit and identification, assessment, monitoring and mitigation of the risks of violation, non-implementation and avoidance of asset freezing decisions as well as advanced controls for the implementation of relevant designations within the scope of PF Law (RoC, art. 7(1)).

c) VASPs are part of the entities obliged to establish a compliance programme (RoC, art. 4(1)(ı)), namely to establish a risk management policy by taking into account their business size, business volume and the nature of the transactions they conduct within the scope of the institutional policy

(RoC, art. 5). VASPs are also required to conduct risk identification, assessment, monitoring and mitigation efforts for the risks of breach, non-implementation and avoidance of asset freezing orders under TF Law No. 6415 and PF Law No. 7262, as well as enhanced controls for the implementation of such sanctions, (RoC, art.7).

Criterion 15.4

a)

i. VASPs defined as "platforms, crypto asset custody service providers, and other organisations designated for provision of other services regarding crypto assets, also including the initial sales or distribution of crypto assets", are required to be licensed by the Capital Market Board (CMB) which will also determine the business activities they are allowed to carry out (Law 6362, art. 35/B(1)).

ii. VASPs are required to be established "in the form of a joint stock company" (Communiqué III-35/B.1, art. 5(1)a). Hence, a VASP can only be legal person in Türkiye and this sub-criterion does not apply.

b) Competent authorities take the necessary legal measures to prevent criminals or their accomplices from being the founders, shareholders, beneficial owner (Communiqué III-35/B.1, art. 6) or holding a management function (Communiqué III-35/B.1, art. 13 - 15) in a VASP.

Criterion 15.5

VASP can only be legal persons in Türkiye. Authorities can apply appropriate sanctions to any natural and legal persons that carry out VASPs activities without the requisite license from CMB (Law 6362, art. 99, 99A and art.109). Authorities shall cancel the application for registration of any VASP presenting non-conformity to the establishment conditions (Communiqué III-35/B.1, art. 5 and provisional art. 1). As of the end of the onsite visit the grace period for operating VASPs to obtain a licence was still ongoing (see IO.3), but Türkiye has the framework to take action against unlicensed VASPs.

Criterion 15.6

a) VASPS are required to be licensed by the CMB which will also determine the business activities they are allowed to carry out (Law 6362, art. 35/B). MASAK regulates and supervises the AML/CFT obligations of FIs through the examiners from different agencies assigned to carry out supervision (Law 5549, art. 11), see Rec. 26. Since VASPs are considered as FIs in Türkiye (RoM, art. 3(1)(f)), they are also subject to AML/CFT regulation and risk-based supervision.

b) MASAK possesses the supervisory powers to supervise VASPs, given that they have been included as FIs under MASAK' supervision and considering Türkiye's rating on R. 27 is LC.

Criterion 15.7

When VASPs were designated as obliged entities in May 2021, MASAK issued guidance on the "Fundamental Principles regarding Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Obligations for VASPs". Moreover, an updated "STR Guidance Specific to the VASP Sector", was published in 2024. MASAK organised a workshop in November 2024 on "Combating ML and TF for VASPs" with the participation of 48 VASPs.

Criterion 15.8

a) VASPs are considered as FIs in Türkiye (RoM, art. 3(1)(f)), hence they are subject to the sanctions that apply to FIs that fail to comply with AML/CFT requirements (Law 5549, art. 13). The sanctions are dissuasive and proportionate with fines being increased by the revaluation rate at the beginning of each calendar year (Law 5549, art. 28). The minor deficiency in R.35 regarding the existence of an eight-year statute of limitations for administrative fine (Law 5549, art. 13(6)) has a minor impact on this sub-criterion.

b) The member of the board of directors or else the senior manager in charge, who do not comply with the obligations shall be given the one fourth of the administrative fine imposed on the obliged party (Law 5549, art. 13(3)).

Criterion 15.9

As FIs, VASPs are required to comply with the requirements set out in Recommendations 10 to 21. Therefore, VASPs regulations reflect the same framework assessed in R.10 to 21 for FIs, the same strengths and weaknesses within the framework also apply to VASPs.

a) VASPs are required to establish a business relationship in the form of a contract with their customer prior to conducting any transaction (Communiqué III-35/B.1, art. 22(1)). In addition, VASPs shall identify their customers or those who act on behalf or for the benefit of their customers by receiving their identification information and verifying it and take necessary measures for revealing the beneficial owner when the amount of a single transaction or the total amount of multiple linked transaction is above 15000 TRY (approx. 411 EUR) (RoM, art. 5(1)(c)).

b) Türkiye applies a de minimis threshold. For virtual assets transfers of 15.000 TRY (approx. 344 EUR) and above intermediated by VASPs, it is required that the following information of the originator is included in messages a) name and surname, title of the legal person registered to trade registry, full name of the other legal persons and unincorporated organisations; b) wallet address, or reference number of the transaction when there is no wallet address; c) at least one of the information defining the originator such as address, date and place of birth, customer number, citizenship number, passport number, or tax ID number. The information of the originator shall be verified. It is required that the information a) and b) above of the beneficiary are included in the virtual asset transfer and the verification of this information is not mandatory (RoM, art. 24/A (1)).

For virtual assets transfers under 15.000 TRY (approx. 344 EUR), VASPs should include information of the originator, and the beneficiary listed in a) and b) above but the verification of this information is not mandatory (RoM, art. 24/A (2)).

As obliged entities, VASPs are required to retain documents, books and records, identification documents and records kept in all forms regarding their transactions and obligations for eight years (RoM, art. 46) and make it available to MASAK (RoM, art. 31).

a) Beneficiary VASPs obtain the information a) and b) above on the originator and the beneficiary as it is included in the VA transfer message (RoM, art. 24/A). Since VASPs licensed in Türkiye are compelled to conduct customer identification prior to conducting any transaction with a new customer (see 15.9.a above), the beneficiary VASP licensed in Türkiye verifies the beneficiary information. VASPs hold this information and have to make it available on request to appropriate authorities (see above, RoM, art. 46 & 31).

b) VASPs should take measures if they receive a VA transfer message that does not contain required information, such as returning, refusing the VA transfer and restricting or ceasing the business relationship (RoM, art. 24/A (3). When receiving VA transfers from an unhosted wallet address or a foreign VASP, VASPs licensed in Türkiye should at least obtain one information defining the originator (RoM, art. 24/A (6) & (7)). However, the requirement to have risk-based policies and procedures for addressing wire transfers is not fully met.

c) Any organisations engaged in any one or more of virtual asset trading initial sales or distribution, exchange, transfer and custody services and operations required therein for, and other transactions that may be identified in relation therewith is considered as a VASP under Türkiye Law (Law 6362, art. 3). Consequently, any FI that would be sending or receiving VA transfers on behalf of a customer would be subjected to VASP regulation.

Criterion 15.10

Pursuant to criterion 6.5(d) and 6.6(g), decisions on freezing and unfreezing are published in the Official Gazette and are considered as notified on the date of their publication (Law 6415, art 11). MASAK notifies immediately the decisions of freezing to any natural and legal persons, public institutions and organisations to whom notification is deemed necessary (RoTF, art. 14(1)(e)) and urgently notifies the repealing decisions to the persons, organisations and institutions which implement the freezing decisions (RoTF, art. 14(4)). There is no restriction to the application of those provisions for VASPs.

Pursuant to criterion 6.5(e), natural and legal persons and public institutions implementing freezing decisions are required to report to MASAK, within 7 days, the asset records (Law 6415, art. 12(5) and RoTF, art. 14.2 and 14.3). There is no restriction to the application of those provisions to VASPs.

Pursuant to criterion 7.2(d) and 7.4(d), freezing decisions or prohibition decisions and decisions repealing such decisions shall be published without delay by relevant public institutions on their websites upon their publication in the Official Gazette (Law 7262, art. 3(3)). In addition, MASAK notifies immediately the decisions of freezing to any natural and legal persons and public institutions to whom notification is deemed necessary (RoPF, art. 11(1)(e)) and urgently notifies the repealing decisions to the persons and institutions which implement the freezing decisions (RoPF, art. 11(4)). There is no restriction to the application of those provisions to VASPs.

Pursuant to criterion 7.2(e), natural and legal persons and institutions are required to report to MASAK, within 7 days, the asset records related to the designations of relevant UNSCRs (RoPF, art. 11(2) and 11(3)). There is no restriction to the application of those provisions to VASPs.

Pursuant to criterion 7.3, MASAK supervises the implementation of asset freezing decisions in relation to PF (RoPF, arts. 17(1) and 17(2)). There is no restriction to the application of those provisions to VASPs.

Criterion 15.11

VASPs are considered as FIs in Türkiye (RoM, art. 3(1)(f)) and have been designated as obliged entities (RoM, art. 4(1)(ü)) with MASAK as their supervisor for AML/CFT obligations (Law 5549, art. 11). There is no restriction for Türkiye to apply to VASPs all forms of international co-operation laid out in Rec. 37 to 40 and for which Türkiye is C/LC.

> ***Weighting and conclusion –*** Türkiye has conducted risk analyses of VA and VASPs to identify ML/TF risks. VASPs are considered as financial institutions in Türkiye and require a license to operate. MASAK supervises their compliance with national AML/CFT requirements. As FIs, VASPs are required to comply with the requirements set out in Recommendations 10 to 21. Therefore, VASPs regulations reflect the same framework assessed in R.10 to 21 for FIs, the same strengths and weaknesses within the framework also apply to VASPs. There are proportionate and dissuasive sanctions in line with R.35 (rated LC). For VAs transfers, VASPs are required to obtain and hold originator/beneficiary information as per the requirements of the Methodology. Those are considered minor shortcomings in light of the materiality of the VASP sector in Türkiye. Recommendation 15 is rated **largely compliant.**

Recommendation 16 – Wire transfers[74]

In its 2019 MER, Türkiye was rated largely compliant with R.16 because of lack of explicit requirements for MVTS providers to consider information on both originator and beneficiary sides to determine whether an STR has to be filled and implementation of targeted financial sanctions.

Originator's financial institutions

Criterion 16.1

FIs are required to verify the identity of customers when the amount of a single transaction or the total amount of linked transactions in wire transfers is equal to or more than TRY 15 000 (EUR 411): art. 5(1) of the ROM. In addition, FIs that send wire transfers are required to verify information regarding the originator (namely the name, surname, title of the legal person registered at the trade registry, the full name of other legal persons and unincorporated organisations; the account number or, where there is no account number, the reference number of the transaction; the address or place and date of birth or at least an identity number such as a passport or tax number for identifying the client): art. 24(1) of RoM. Banks are not permitted to make remittances for customers who have not provided their identity and tax number: art. 76 of Law No 5411.

a) Concerning originator information:

   Specified information on originators must be included in wire transfers: art. 24 of the RoM. This includes the name of the originator.

   This also includes a requirement for a transaction reference number but not for the transaction reference number to be unique or to permit traceability of the transaction (although in practice this is the case). Since November 2018, a Unique End-to-End Transaction Reference Number (UETR) has been required by the CBRT Payment Systems Message Structures and Operation Types, (Message Standards in short), which is an attachment of the operational, enforceable rulebook (see (b) below), to be included in messages, permitting traceability of each transaction.

b) The relevant information is required. Specified information on beneficiaries must be included in wire transfers; (RoM, art. 24.) Concerning beneficiary information, a specific transfer message of the CBRT payment systems is used for TRY cross-border payments:

   The CBRT Payment Systems Message Structures and Operation Types (an operational rulebook (updated on November 2024) (Annex on Message Structures and Operation Types - R.16.1-1) attached to the CBRT Systems Operational Rulebook (updated in March 2023) (Annex on operational rulebook - R.16.1-2) made under Law 1211, Law 6493 and the Regulation on Payment and Securities Settlement Systems Activities) requires the name of the beneficiary to be included on messages.

   The CBRT operational rulebook also requires inclusion of the beneficiary's account number. Since November 2018 the Message Standards has required a UETR to be included in messages.

Criterion 16.2

The RoM does not explicitly refer to batch files. However, the provisions specified in c.16.1 apply to all cross border wire transfer equal to or more than TRY 15 000 (EUR 411) whether they are processed in batch files or not.

[74]This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

Criterion 16.3

Türkiye applies a de minimis threshold, in this scope, FIs are required to ensure that all cross-border wire transfers below the threshold of TRY 15000 (EUR 411) are always accompanied with the required originator and beneficiary information. (RoM ; art. 24(2))

Arts. 24 (originators) and 25 (beneficiaries) of the rulebook (CBRT Systems Operational Rulebook) require wire transfers to include information regarding the originator/beneficiary (name, surname/business title and identity number or taxpayer identification number) irrespective of the threshold of TRY 15 000 (EUR 411): art. 5(1) of the RoM.

Criterion 16.4

The information mentioned in criterion 16.3 need not be verified for accuracy (RoM, art. 24(2)). On the other hand, FIs are required to verify the identity of customers (and those persons who act on their behalf or for their benefit) in cases requiring a STR regardless of the monetary amount involved (art. 5(1)(d) of the RoM. The customer can be considered to be the originator.

Criterion 16.5

See c.16.1 for the obligations on which information should be included on originator as part of a wire transfer. These provisions also apply to domestic transfers.

Criterion 16.6

As indicated above, the relevant information accompanies the wire transfer.

Criterion 16.7

The ordering FI is required to maintain all originator and beneficiary information collected for a period of eight years, in accordance with Recommendation 11: art. 8(1) of the Law No.5549.

Criterion 16.8

The provisions of the ROM and Law No 5549 specified in c.16.1 are obligatory. Therefore, it is not allowed to execute the wire transfer, if it does not comply with the requirements specified at criteria 16.1-16.7.

Intermediary financial institutions

Criterion 16.9

FIs intermediating the transfer shall include the information regarding the originator in the wire transfer message, in the message chain where the transfer order is made to the FI that will execute the payment, and are required to pay special attention to transfer this information at every stage of the transfer (RoM, art. 24(6))

Criterion 16.10

See c.16.9 for the provisions on intermediary institutions. The Turkish authorities have advised that all FIs taking part in a wire transfer chain are required to ensure that the relevant information accompanies the wire transfer, that under art. 8(1) of Law 5549 requires information to be retained for eight years and that there is no possibility at the technical level for information not to accompany a transfer. In addition, under art. 14-ç of the CBRT Payment Systems Operational Rulebook, the CBRT is obliged to retain information on messages processed by the system for a period determined by law and, in case of dispute, to provide the records to relevant parties and authorities. Also, under art.17-e the FI is obliged to keep all information for eight years. In addition, under art. 23 of Law No.6493, documents and records should be kept a period of minimum ten years.

Criterion 16.11

In the event that a FI receives a wire transfer message, which does not include required originator information (see c.16.1), either it must return the wire transfer, or it must complete the missing information through the FI who sent the message: RoM, art. 24(4). In addition, all financial institutions intermediating the transfer are required to include the information regarding the originator in the wire transfer messages and pay special attention to transfer this information at every stage of the transfer. (RoM, art. 24(6)) (Please see the explanation in c.16.9).

Criterion 16.12

See c.16.9 to 16.11. Art. 15 applies monitoring and controls to information required to be placed in wire transfer messages, completing the missing information and updating the messages. Besides, article 24 of the ROM as regards originator and beneficiary information and the wider provisions in the ROC and ROM address the requirements.

Beneficiary financial institutions

Criterion 16.13

See c.16.11 and 16.12. In the event that a beneficiary FI receives a wire transfer message, which does not include required originator information (see c.16.1), either it must return the wire transfer or it must complete the missing information through the FI who sent the message (art. 24(4) of the RoM). Similar requirements apply for the beneficiary information as per the CBRT Standards.

Criterion 16.14

Art. 5(1) of the ROM provides that FIs must identify their customers or those who act on behalf of or for the benefit of their customers by receiving their identification information, verifying it when the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than TRY 15 000 (approx. EUR 411) in wire transfers and maintain this information in accordance with R.11.

Criterion 16.15

The framework does not include specific language addressing the criterion. However, the provisions and argumentation from c.16.11 onwards mitigate the absence of explicit language in meeting this criterion.

Money or value transfer service operators

Criterion 16.16

Art. 3 and 4 of the ROM apply the provisions of that instrument to MVTS providers. Under art. 4(1) the provisions apply to FIs and their branches, agencies, representatives, commercial proxies and similar affiliated units. Under art. 4(2) the provisions apply to branches, agencies, representatives, commercial representatives and similar affiliated units in Türkiye of a head office abroad. Under art. 4(3), the provisions extend to branches, agencies, representatives, commercial representatives and similar affiliated units of head office in Türkiye, when they operate abroad. Affiliated units include agents. The provisions of art. 4(3) apply to the extent that the legislation and competent authorities of the foreign jurisdiction allow.

Criterion 16.17

See c16.16. The requirement to report suspicion is analysed in R.20. Under art. 31 of the ROC compliance officers must evaluate information and findings obtained through research that he/she has carried out to the extent of his/her power as well as the possibility of suspicion. Necessary information and documents must be requested from all units of the FI. There is no language explicitly covering the requirement of the criterion that information from both ordering and beneficiary sides should be taken into account to

determine whether an STR has to be filed. However, the requirements of the ROC mentioned above mean that compliance officers would take into account information from the ordering and beneficiary sides of a wire transfer automatically.

Implementation of targeted financial sanctions

Criterion 16.18

The provisions analysed in c.6.4 and 6.5 apply to wire transfers.

> ***Weighting and conclusion –*** There are minor gaps regarding lack of explicit requirements for MVTS providers to consider information on both originator and beneficiary sides to determine whether an STR has to be filed and implementation of targeted financial sanctions. Recommendation 16 is rated **largely compliant.**

Recommendation 17 – Reliance on third parties[75]

In its 2019 MER, Türkiye was rated compliant with R.17.

Criterion 17.1

Reliance on third parties is covered within the ROM and in a guidance paper issued by MASAK entitled "The Principle of Reliance on Third Parties". FIs can establish business relationships or carry out transactions by relying on measures taken by another FI concerning the identification of the customer, the person acting on behalf of the customer, the beneficial owner, and information on the purpose of the business relationship or transaction: ROM, art. 21. In such circumstances, the responsibility remains with the FI relying on the third party.

a) Art. 21(3) provides that the FIs establishing a business relationship or conducting a transaction by relying on third party shall immediately receive identity data on the customer from the third party. The concept of identification data includes all of the information collected on the relationship/transaction specified in chapter 3 of the ROM; in essence, this is all CDD information required by the ROM.
b) Reliance on third parties is only permissible if
   - the third parties have taken other measures which will meet the requirements of record keeping and the principles of customer due diligence: ROM, art. 21(2)(a)
   - certified copies of documents relating to customer identification from the third party are made available immediately when requested: ROM, art. 21(2)(b).
   - Customer identification of a customer whose information is shared by a third party has not been done under simplified measures RoM, art. 21(2)(c).
c) FIs are required to ensure that third parties are subject to regulation and supervision in accordance with international standards: RoM, art. 21(2). In addition, under the same article, reliance is only possible when the FI ensures that the third party has taken measures that meet the requirements of customer identification, record keeping and the principles of CDD. Paragraph V of the guidance paper issued by MASAK provides that it should be ensured that the third party has taken necessary measures within the scope of CDD, particularly, customer identification; that it is subject to regulations and supervisions compatible with international AML/CFT standards.

[75] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

Criterion 17.2

Reliance on third parties is possible if the parties are residents abroad only if it is ensured that third parties have met a set of measures (e.g. customer identification, record keeping and customer due diligence), and are also subject to AML/CFT regulations and supervision in accordance with international standards: ROM, art. 21(2)(a). Reliance on third parties cannot be applied in cases where the third party is resident in a risky country: ROM, art. 21(5).

Criterion 17.3

There are no specific provisions for FIs that rely on a third party that is part of the same financial group. Instead, the same legal provisions that govern third party reliance are applicable: ROM, art. 21:

a) CDD and record keeping requirements and programs against ML/TF are applied (see criterion 17.1)
b) The implementation of these measures is supervised by a competent authority (see criterion 17.1).
c) Reliance on third parties cannot be applied in cases where the third party is resident in a risky country (see criterion 17.2).

Weighting and conclusion – All criteria are met. Recommendation 17 is rated **compliant.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries[76]

In its 2019 MER, Türkiye was rated partially compliant with R.18 and re-rated to largely compliant in its 2021 FUR.

Criterion 18.1

Banks[77] , capital market companies, insurance and pension companies, group A exchange offices listed in the foreign exchange legislation, electronic money and payment institutions, and the General Directorate of Post (in relation to its banking activities) are required to establish a compliance programme for AML/CFT purposes (RoC, art. 4). The compliance programme is risk-based and must ensure compliance with laws, regulations and communiques. It includes the development and implementation of institution-wide policies and procedures, risk management activities, monitoring and control activities, training activities, and internal audit (RoC, art. 5(1)). When developing risk management policies, FIs must take into account the business size, business volume and the nature of transactions conducted (RoC, art. 11). The purpose of the policy is to grade, monitor, assess and reduce the risk exposure of obliged entities.

There are additional requirements in some sector specific legislation. Payment institutions are required to set up internal control methods and to monitor their agents to fulfil AML/CFT requirements and prevent fraud (ROP, art. 13(6)). Group A exchange offices – those having a higher variety of activities and business volume (equity, size of assets, number of employees and branches, etc) - are required to establish an effective internal control system, including a risk management system, in order to continuously check, audit and detect errors, fraud and irregularities with regard to all activities and prevent them (Communique 2018-32/45, art. 15(3)).

a) Banks, capital market intermediaries, insurance and pension companies and General Directorate of Post (for banking activities) are required to appoint a compliance officer and establish a compliance unit, with the executive being responsible for appointing the assigning the compliance officer and the unit (ROC, arts. 5(1) and 6(2)). The compliance officer reports to the executive board or to one

[76]This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019 and FUR 2021, with minor non-substantive edits included from Türkiye.

[77]Excludes the Central Bank of the Republic of Türkiye and Development and Investment Banks.

or more members of the board to whom the board has transferred its authority (ROC, art.16). Other FIs are required to appoint a compliance officer at administrative (i.e. managerial) level.

b) Compliance officers are required to not have committed serious crimes (ROC, arts. 17 and 30). In addition, there are educational requirements, citizenship requirements, managerial experience requirements and requirements to prevent a conflict of interest. The requirements cover only compliance officers and not all employees as required in the criterion. The gap is reduced by supervisory approaches (as opposed to what is required of FIs), as there are requirements for employees at managerial level to be fit and proper through the mechanisms identified at R.26. In addition, the Communiqué on Principles Regarding Licensing and Recordkeeping for Those Engaged in Capital Market Activities (VII-128.7) (Annex-1), requires persons working in publicly-held joint stock companies and capital market institutions to have qualifications.

c) FIs are required to carry out training activities, based on a training policy: ROC, arts. 5(1) and 21. The policy must include the realisation of training activities, the determination of which staff will be trained and training methods. Art. 22 onwards cover training activities, training subjects, reporting of training results to MASAK and training by MASAK. Training activities must be reviewed and repeated periodically according to necessity (art. 22(3)). Annual internal audit reviews must cover whether training activities are sufficient and efficient: ROC, art. 26.

d) Annual internal audit reviews are required: ROC, arts. 26 and 27. Deficiencies found as a result of internal audit must be reported to the executive board. It is not explicit that the internal audit function must employ/use staff not used in other functions and therefore that the units be separate to other functions. This is mitigated by the responsibilities placed on the internal audit function and reporting to the executive board. For most but not all types of FI there are provisions in instruments other than the ROC which suggest independence of the internal audit function. Under art.32 of Banking Law 5411 the internal audit units of banks must perform their functions in an impartial and independent manner. Under art. 3 of the Communique on Principles Regarding the Internal Auditing Systems of Brokerage Houses, internal audit must be conducted independently from the routine operations of the brokerage house. Under art. 13 of the communique on Portfolio Management Companies and Activities of Such Companies, there must be an inspection unit independent from the daily activities of the company, employing inspectors working solely and exclusively in the unit, and reporting directly to and responsible to the Board of directors. Under art. 4 of the Regulation on Internal Systems of Insurance, Reinsurance and Pension Companies, internal audit shall report directly to the Board of directors and be administratively independent.

Criterion 18.2

Türkiye' requires financial groups to establish group-wide AML/CFT programmes – including training, internal audit, control and risk management systems, (Article 5 (1) of AML Law). Further, Article 5(2) of the AML Law enables the sharing of information on customers, accounts, and transactions within a financial group. In order to implement group wide compliance programmes, the compliance officer of the parent financial institution is also determined as the compliance officer of the financial group. Within this scope, compliance officer of the financial group is required to:

a) to work as necessary in order to ensure compliance of the financial group with the Law (AML Law) and the regulations issued pursuant to it at the group level and to ensure the necessary communication and co-ordination with MASAK,

   to establish the policies and procedures of the financial group and submit the group's policies to the approval of the executive board,

b) to establish the risk management policy of the financial group, to carry out risk management activities,

c) to establish the monitoring and control policies of the financial group and to carry out related activities,

d) to share the issues that are determined to be risky as the result of risk management, monitoring and control activities with the relevant financial institution within the group,

e) to establish the information sharing policy of the financial group and to take necessary measures to securely share this information within the group and

f) to co-ordinate the training program of the financial institutions affiliated to the group in order to prevent laundering the proceeds of crime and financing of terrorism and to pay attention to the effective implementation of training programs ROC art. 20/A (2).

Furthermore, institutions within the group can share information relating to customer due diligence, accounts and transactions in order to ensure that the measures in the scope of the compliance programme are implemented at the group level: RoC, Article 20/B (1). Those who work in financial institutions within the group may not disclose the information received within the scope of their duties and may not use them for the benefit of themselves or third parties. The compliance officer of the group is responsible for taking necessary measures to securely share information within the group. This responsibility is also shared with compliance officers and executive boards of the financial institutions within the group: ROC, art. 20/B (3).

While the financial institutions within the group may not share on the fact that an STR has been submitted (ROC, art. 20/B (4)), there is no provision that prevents sharing of underlying information. However, there are no explicit requirements as set out in the criterion in respect of group-wide implementation of AML/CFT programmes and sharing of information by group level functions with branches and subsidiaries when relevant and appropriate to risk management.

With regard to the confidentiality of information exchanged, financial group's compliance officer is responsible to establish the information sharing policy of the group and to take measures to securely share the information ROM art. 20/A(2). Those who work in institutions within the group, may not disclose the information they have learned within the scope of information sharing and may not use them for the benefit of themselves or third parties.

Criterion 18.3

Foreign branches, agencies, representatives, commercial representatives and similar affiliated units are required to implement AML/CFT measures consistent with the requirements under Turkish law to the extent that the legislation and authorities of the other country permit: ROM, art. 4(3). Majority-owned subsidiaries are deemed to be covered within the notion of 'similarly affiliated units'.

Under art. 40(2) of the ROM, individuals within obliged parties with inspection authority provided by legislation (i.e. compliance officers and internal audit officers) should, through their units, inform MASAK of breaches.

Additionally, if the legislation of relevant country does not permit the implementation of the measures within the scope of the compliance program, MASAK has to be informed of this situation and additional measures have to be taken ROC, art. 4 (3).

> ***Weighting and conclusion –*** Minor deficiencies remain. Notably there is no legislative requirement for groups to have policies and procedures for sharing information within groups. There are also no requirements for financial groups to apply additional measures and inform home supervisors if the host country does not permit the proper implementation of AML/CFT measures. However, the impact of these deficiencies is largely mitigated through other measures. For example, the RoM requires compliance officers to inform MASAK where an obliged entity breaches AML requirements which in practice means financial groups should be informing home supervisors of potential issues with implementation of AML/CFT measures. Recommendation 18 is rated **largely compliant.**

Recommendation 19 – Higher-risk countries[78]

In its 2019 MER, Türkiye was rated largely compliant with R.19 because of no explicit obligation for financial institutions to apply enhanced due diligence measures for countries when called upon by the FATF, unless such countries are defined as high-risk by the Ministry of Treasury and Finance.

Criterion 19.1

Risky countries are defined by the Ministry of Treasury and Finance as countries which do not have sufficient AML/CFT laws and regulations, do not co-operate on combating ML/TF or are considered risky countries by competent international organisations (RoM, art. 3). Where the FATF identifies a country as having ML/TF risks, a decision by the Ministry of Treasury and Finance is required for that definition and its implications to have effect in domestic law. Obliged entities are required to pay special attention to business relationships and transactions with natural or legal persons, unincorporated organisations and citizens located in risky countries (RoM, art. 25). One or more enhanced measures are required under two circumstances: i) transactions within the scope of arts. 18, 20 and 25 and ii) high-risk situations identified in the framework of the implementation of the RBA (RoM, art. 26/A). RoC art.3 also requires enhanced measures for high-risk customers. Nevertheless, a gap exists due to lack of an explicit provision for FIs to take enhanced measures when called upon by the FATF unless defined by the Ministry.

Criterion 19.2

Türkiye is able to label countries as high-risk, triggering enhanced due diligence measures, when called upon to do so by the FATF and independently of any call by the FATF to do so, through the mechanism at the Ministry of Treasury and Finance (see criterion 19.1). In addition, the Ministry is authorised to determine other enhanced measures as needed (which could include countermeasures) (RoM, art. 26A(2)).

Criterion 19.3

See c.19.1 and 19.2 and the ability of the Ministry of Treasury and Finance to define risky countries. MASAK is required to co-operate with domestic institutions and exchange information in the fulfilment of its duties: Presidential Decree No. 1. MASAK places information on its website about public statements made at FATF plenaries on the weaknesses in the AML/CFT systems of other countries. To-date web traffic indicates that obliged entities regularly visit the MASAK's website, particularly FIs. It also organises periodic meetings with representatives of the private sector.

> ***Weighting and conclusion –*** There is no explicit obligation for financial institutions to apply enhanced due diligence measures for countries when called upon by the FATF, unless such countries are defined as high-risk by the Ministry of Treasury and Finance. Recommendation 19 is rated **largely compliant**.

Recommendation 20 – Reporting of suspicious transactions[79]

In its 2019 MER, Türkiye was rated compliant with R.20.

Criterion 20.1

Obliged entities are required to report to the FIU of any transaction when any information, suspicion or reasonable grounds to suspect that the asset, subject to the transactions, is acquired through illegal ways

[78]This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019.

[79]This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

or used for illegal purposes (Law 5549, art.4). Law sets forth the STR requirement in general framework, the scope of STR obligation related to TF is wider in the ROM where the suspicion includes assets suspected to be used for terrorist activities or by terrorist organisations, terrorists or those who finance terrorism (ROM, art.27). The reporting must be made within 10 days when the suspicion occurred (ROM, art. 28(2)). Any new information in relation to the reported transactions must be addressed to the FIU without delay (ROM, art. 28(3)).

Criterion 20.2

Obliged entities are required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction (ROM, art. 27(1)(2)).

> ***Weighting and conclusion –*** All criteria are met. Recommendation 20 is rated **compliant**.

Recommendation 21 – Tipping-off and confidentiality[80]

In its 2019 MER, Türkiye was rated compliant with R.21.

Criterion 21.1

Natural and legal persons are protected by law from both civil and criminal liability for fulfilling their reporting obligations (Law 5549, art. 10(1)). The compliance officers, legal representatives of the obliged entities, their managers and personnel complying with the obligation of reporting suspicious are protected by the regulation (RoM, art. 29(4)). While no explicit requirement that the reporting should be made in good faith in the legislation and the regulation, there is a general requirement regarding good faith in TCL and Turkish Civil Law.

Criterion 21.2

Obliged entities are prohibited by law from disclosing the fact that an STR or related information is being field with the FIU except to supervisors and courts (Law 5549, art. 4(2)). The general provision about the prohibition of this disclosure is set in the law. The extension of prohibition covering the directors, officers and employees of FIs is regulated in the regulation (RoM, art. 29(1)(2)).

> **Weighting and conclusion –** All criteria are met. Recommendation 21 is rated **compliant**.

Recommendation 22 – Designated non-financial businesses and professions (DNFBPs): customer due diligence[81]

In its last MER, Türkiye was rated partially compliant with these requirements and has been re-rated largely compliant in its 2023 FUR. The minor deficiencies identified in R.10 still had an impact on this Recommendation.

Criterion 22.1

In Türkiye, casinos are forbidden (Law 4302). Real estate agents, dealers in precious metals and stones, notaries, lawyers, accountants and independent audit institutions are defined as "designated non-financial businesses and professions" (RoM, art. 3/1(m)) and they fall into the category of obliged entities (RoM, art. 4/1). TCSPs do not exist as a separate category in Türkiye, nevertheless, accountants and lawyers, who are most likely providing professional services to its clients including professional trustees based on trust

[80]This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

[81]Recommendation 22 is assessed considering legislative and regulatory changes in Türkiye.

agreements founded according to the laws of foreign countries, are designated as obliged entities. Other DNFBPs are required to comply with the CDD requirements set out in R. 10 in the following situations:

a) Real estate agents when they buy and sell immovables for trading purposes and intermediaries of these transactions (RoM, art. 4(1)(n)).
b) Dealers in precious metals and stones (RoM art. 4(1)(k)).
c) Notaries (RoM art. 4(1)(s)).
d) Accountants (RoM art. 4(1)(t)).
e) Independent audit institutions, which is authorised to conduct audit in financial markets (RoM, art. 4(1)(u)).
f) Lawyers are covered for the activities of i) buying and selling of real estate; ii) managing of client money, securities and other assets; iii) management of bank, savings or securities accounts and iv) creation, operation or management of companies. Lawyers are also covered in terms of CDD requirements for establishing, merging, managing, transferring and liquidating a company, foundation and association (Law 5549, art.2(1)(d))

The deficiencies identified under R.10 for relevant criterions 10.5, 10.6, 10.8, 10.9, 10.10, 10.11, 10,19 and 10.20 also apply to DNFBPs. These were considered as minor deficiencies (R.10 rated LC in 2019 MER).

Criterion 22.2

DNFBPs are required to comply with record keeping obligations as described in R.11, including keeping records for eight years (Law 5549, art.8; ROM, art. 46).

Criterion 22.3

DNFBPs are required to comply with the same PEPs requirements as FIs (Com. 21), see R.12 analysis.

Criterion 22.4

DNFBPs are required to specially consider the risks posed by new and developing technologies, existing and new products including new delivery channels, and new business applications for ML/TF and take appropriate and effective measures against them (RoM, art.20). In addition, DNFBPs should apply, in proportion to the identified risk, one or more enhanced measures (RoM, art. 26/A) and measures for high-risk situations they identify (RoM, art. 25). DNFBPs have to carry out monitoring and controlling activities in order to ensure compliance with the obligations imposed by the Law, regulations and communiques issued pursuant to the Law, for defining, monitoring and mitigating risks by taking into account the risks identified within the scope of training, monitoring and national risk assessment, and to take the necessary measures within this scope (which includes new technologies and developing technologies, existing and new products including new delivery channels, and new business applications for ML/TF) (RoC, art. 32/A).

Criterion 22.5

DNFBPs are not allowed to rely on third parties while conducting transactions (RoM, art.21).

> ***Weighting and conclusion –*** The deficiencies identified under R.10 for relevant criteria 10.5, 10.6, 10.8, 10.9, 10.10, 10.11, 10,19 and 10.20 also apply to DNFBPs. These are considered as minor deficiencies (R.10 rated LC). Recommendation 22 is rated **largely compliant**.

Recommendation 23 – DNFBPS: other measures[82]

Türkiye was rated partially compliant with R.23 in its 2019 MER and re-rated compliant in its 2022 FUR. Lawyers were not covered and there were no specific requirements for DNFBPs to comply with internal control and high-risk country requirements.

Criterion 23.1

As obliged entities, DNFBPs are required to comply with STRs requirements (Law 5549, art. 4).

Criterion 23.2

DNFBPs are required to carry out monitoring and controlling activities to comply with internal control requirements set out in Recommendation 18 (RoC, art. 32A).

Criterion 23.3

DNFBPs are required to pay special attention to business relationships and transactions with natural and legal persons, located in risky countries and to obtain information about the purpose and the nature of the transactions (RoM, art. 25). Risky countries are defined as countries which do not have sufficient AML/CFT laws and regulations, do not co-operate on combating ML/TF or are considered risky countries by competent international organisations (RoM, art. 3 (i)). Obliged entities should apply one or more enhanced measures are required under two circumstances: i) transactions within the scope of arts. 18 (complex, unusual large transactions and no apparent legitimate economic purpose), 20 (non-face-to-face transactions) and 25 (risky countries) and ii) high-risk situations they identify in the (ROM, art. 26/A). However, as for FIs, DNFBPs are not required to apply EDD to business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF unless such countries are defined as high-risk by the Ministry of Treasury and Finance. (see R.19).

Criterion 23.4

DNFBPs are required to comply with the same tipping-off and confidentiality requirements as FIs. So the analysis in relation to R.21 equally applies to DNFBP.

> *Weighting and conclusion –* There is a minor deficiency in relation to DNFBPs having to comply with the higher-risk countries requirements set out in Recommendation 19. Recommendation 23 is rated **largely compliant**

Recommendation 24 – Transparency and beneficial ownership of legal persons[83]

In its 2019 MER, Türkiye was rated partially compliant with R. 24 and through the follow-up process in 2022, was re-rated largely compliant. Minor shortcomings include sanctions, particularly for legal persons, remaining very low and therefore are not dissuasive and only general information about co-operatives and guidelines is publicly available in the KOOPBİS system. Further, the DERBİS system (for associations) and VBYS (for foundations) are only available to public authorities. Türkiye also did not have a mechanism to measure the quality of assistance received from other countries in locating the beneficial ownership (BO) information residing abroad. Türkiye is being assessed following changes to R. 24 which now require countries to: assess the risks of misuse of both domestic and foreign legal persons for ML/TF; use a multi-pronged approach to ensure that the BO information of a company can be determined in a timely manner; ensure that there is no issuance of new bearer shares or bearer share warrants; implement measures to

[82]Recommendation 23 is assessed considering legislative and regulatory changes in Türkiye.

[83]Recommendation 24 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

prevent the misuse of nominee directors and shareholders; and facilitate timely access to BO information by competent authorities.

Scope extends to companies and other legal persons

Criterion 24.1

The requirements hereunder apply to all forms of legal persons in Türkiye, with some gaps related to foreign created legal persons with sufficient links.

Türkiye has a legal framework that defines and regulates different forms of legal persons.

a) *Companies*: (***Met***) Commercial legal persons may take five primary forms: joint-stock companies, limited companies, general partnerships, limited (commandite) partnerships and co-operatives (Turkish Commercial Code (TCC), art. 124). The TCC provides the legal basis for the formation, structure and operation of these companies (except co-operatives, which are regulated under the Co-operatives Law, Law No. 1163). All entities are subject to the same registration, reporting and beneficial ownership (BO) requirements.

b) *Foundations, Anstalt and Waqf: (**Met**)* Foundations are formed under the Civil Code (art. 101) and further governed by the Foundations Law, Law No. 5737. There are no entities deemed 'Anstalt' in Türkiye. There is no separate category of 'Waqf' as 'Waqf' are referred to as '*foundations*' in Türkiye. Limited liability partnerships are established under the TCC and must register in the Trade Registry (MERSİS), where information on their ownership, management and principal office is recorded and made publicly available. As corporate taxpayers under the Corporate Tax Law (Law No. 5520), they are also required to submit BO information to the TRA in accordance with Communiqué No. 529 on the Notification of Beneficial Ownership, with updates required quarterly and within one month of any change. Foundations are governed by the Foundations Law (Law No. 5737) and supervised by the General Directorate of Foundations. Foundations must report prescribed administrative and financial information to the General Directorate with a requirement to collect, maintain, or disclose BO information.

c) *Other types of legal persons:**(Met)*** Associations are governed under the Law on Associations (Law No. 5253) and Civil Code provisions and are required to provide or maintain BO information in line with Communiqué No. 529. They are subject to a comprehensive registration and monitoring mechanism through the DERBİS system, operated by the Ministry of Interior's Directorate General of Civil Society. DERBİS captures extensive basic information on associations, including their founding members, governing board, registered address, fields of activity and details of domestic and foreign funding. Associations are legally required under the Law on Associations to update their records when changes occur—such as amendments to their charter, leadership structure or contact information—and to submit annual activity and financial reports through DERBİS.

d) *Foreign-created legal persons: **(Partly met)*** Türkiye has not taken sufficient measures to ensure that the requirements of criteria c. 24.3 (b) and c. 24.10 are applied by the *competent* authorities to foreign legal entities posing ML/TF risks and which have sufficient links with Türkiye.

Criterion 24.2

Türkiye has mechanisms in place to identify, describe and make publicly available key information regarding legal persons, including their types, creation processes and the collection of basic and BO information. These mechanisms are set out in a series of legislative instruments, including the TCC, the Civil Code and sector-specific laws governing co-operatives, associations and foundations**.**

(a) ***(Met)*** Türkiye recognises five principal forms of commercial legal persons (c. 24.1 refers)**.** Each form is subject to detailed regulation regarding its structure, formation and operational requirements. These frameworks define each legal form, its purpose, governance and obligations. Descriptions of these legal persons and their basic features are publicly available through the Turkish Trade Registry Gazette and official websites such as www.ticaretsicil.gov.tr.

(b) ***(Met)*** The processes for the creation of each type of legal person are outlined in national legislation. For companies and co-operatives, registration with the Trade Registry is required, following submission of a notarised or authorised articles of association. Associations must submit a charter and a declaration of establishment to the local authority, while foundations are established either by deed or testament and acquire legal personality upon court registration. Registration details are published in the Trade Registry Gazette and processed through the electronic MERSIS platform. Co-operative establishment is also supported by KOOP-BIS, an additional registry system.

(c) (***Met***) Türkiye has implemented several mechanisms for collecting and maintaining basic and BO information. Basic information on company shareholders, directors and structure is collected at the time of incorporation and recorded in the Trade Registry and MERSIS. BO information is submitted to the TRA and updated quarterly for corporate taxpayers or annually for others. Changes in BO must be reported within one month. This information is supplemented by data from the CSD and reporting obligations imposed on obliged entities under the AML Law. BO data is also made available to competent authorities and certain elements are publicly accessible through MERSIS and the Trade Registry Gazette TCC art. 354 (Joint Stock Companies); art. 575 (Limited Companies); art. 232 (General Partnership); Law No. 1163, Co-operatives Law, art. 3 (Co-operatives); AML Law No.5549, RoM and Tax Procedure Law General Communique no 529 for BO information); Law No.4721, art. 59 (Associations); and Law No. 4721, art. 102 (Foundations). While Türkiye has established a BO reporting framework under Communiqué No. 529 for entities that are taxpayers under the Tax Procedure Law, this framework does not appear to explicitly extend to certain tax-exempt legal persons, such as some foundations, associations and tax-exempt co-operatives. As a result, these entities are not required under the Communiqué to collect, maintain or submit BO information to the TRA. But enterprises formed by tax-exempt entities are required to report beneficial ownership information. Tax-exempt legal persons are still required to provide detailed information about the composition, key individuals, and detailed information that is housed in KOOPBIS, VBYS, and DERBIS and monitored regularly addressing this gap.

Risk assessment and risk mitigation

Criterion 24.3

In 2025, Türkiye updated its 2021 ML/TF risk assessment of legal persons.

a) (***Met***) Türkiye developed a risk analysis methodology involving six stages and five categories of risk across 31 criteria. This follows on its July 2021 'ML/TF risk assessment of all types of legal persons in Türkiye'. A quantitative assessment was conducted for corporate taxpayers covering the period 2021–2024. The analysis evaluated the following risk factors: cash transactions and money transfers, POS and credit card activity, BO opacity and indicators of forgery in trade. Based on this, joint-stock and limited companies were identified as posing relatively higher risks, with limited companies scoring higher for POS-related risks and joint-stock companies for BO-related risks. The analysis further included associations and foundations, with differentiated measures considered in proportion to risk. Results were disaggregated by region and sector (Statistical Classification of Economic Activities in the European Community (NACE) codes), supporting targeted risk mitigation efforts. The risk assessment also indirectly addressed the use of shell companies as they may relate to the identified risk factors. Geographic distribution and an assessment of legal entity risks under specific industrial sectors that tied into the NRA were also assessed in a detailed manner. Türkiye's

2025 Legal Persons Risk Assessment represents a meaningful step forward in analysing ML and TF risks associated with legal entities, reflecting a data-driven approach and improved inter-agency co-ordination.

b) (***Partly met)*** Türkiye also assessed risks associated with foreign-created legal persons operating within its borders, including limited taxpayers and those with foreign majority ownership. The same methodology was applied to evaluate risks related to inter alia cash transactions, with particular focus given to real estate purchase risk of such companies. The risk assessment does not address the ML/TF risks of foreign legal persons that have sufficient links to the jurisdiction but lack foreign majority ownership and the risks that may be missed through this majority shareholder approach or whether specific higher risk sectors may benefit from lower thresholds or examining the risk based on control through other means. The risk assessment also does not sufficiently distinguish between domestic and foreign created legal persons for TF risk.

Basic information

Criterion 24.4

Türkiye requires that all commercial companies be registered in the trade register (TCC, art. 354, 355 and 588). The Trade Registry is the official registry for this purpose and registration is a mandatory legal requirement for all types of commercial companies. The Trade Registry Gazette publishes all registration details and is publicly accessible online at www.ticaretsicil.gov.tr. The MERSIS system permits multiple legal persons to be registered at the same address, which may limit the usefulness of address information as a risk indicator on its own. The MERSIS system (Central Trade Registry System) is used to record and store all commercial registry transactions electronically, ensuring availability of accurate and up-to-date information. Additionally, any person may inspect the contents of the trade registry and the supporting documents maintained by the registry (TCC, art. 35(2)). All companies are required to have written and notarised articles of association, which must be submitted at registration and contain key details such as: company name and headquarters, scope of activity, capital and shareholding structure as well as identity of shareholders and directors. For co-operatives, similar obligations apply (Co-operatives Law, art. 3). They must register via MERSIS and also report updates through KOOP-BIS, a sector-specific monitoring system accessible to the relevant authorities.

Criterion 24.5

a) All companies in Türkiye are required by law to obtain and record key information at the time of incorporation (TCC art. 335-337 (joint stock companies); TCC art. 575-576 (limited companies); Law No. 116 art. 1-4 (co-operatives); TCC art 212-216 (General Partnerships); Law No. 4721 art. 58-60 (associations); Law No. 4721, art. 102, 101 and 106 and Law No. 5737, art. 6 (foundations)). This information is submitted to the Trade Registry, stored electronically via MERSIS, and publicly accessible through the Trade Registry Gazette. Furthermore, statutory requirements are elaborated in guidance from the Ministry of Trade. The collected information will vary depending on the type of company and includes**:** the articles of association approved by the Ministry of Trade, the signature declaration of the authorised representatives (notarised), the notarised copies of the identity cards of the partners, the commitment letter if capital in kind is contributed, the court-approved expert report and court decision, the receipt showing that a certain payment was deposited as a fund in proportion to the capital amount, if there is a legal person among the founders and the documents containing the decision to participate in the company to be established. Minimum basic information as outlined is collected and recorded for all companies.

b) Türkiye requires companies to maintain an internal share register, in accordance with the TCC's provisions: joint-stock companies must maintain a share register (TCC, art. 499); limited companies are required to keep a share register (TCC, art. 594); and co-operatives must maintain a share book,

with share transfers documented and monitored by the Board of Directors (Co-operatives Law, art. 14). For general and commandite partnerships, there is a requirement to register any changes to matters already registered (TCC, art. 31).

c) The share register must be maintained by the company. Furthermore, there is a mandate for all commercial companies to maintain approved trade books, including the share register, board resolutions and general assembly records (TCC, art. 64–65). These must be notarised prior to commencement of business (TCC art. 335-337). The MERSIS platform complements physical recordkeeping by supporting digital storage and registry accessibility for competent authorities. Information must be recorded accurately, in a timely manner and completely, and is subject to penalties for non-compliance. Companies are sanctioned with administrative fines for failure to maintain required records (TCC, art. 562) and heavier sanctions under the Tax Procedure Law where applicable.

Beneficial ownership information

Criterion 24.6

a) Türkiye requires all legal persons to obtain, hold and update accurate BO information. All companies must maintain internal records, including the share register (TCC art. 499 and 594). These records capture shareholding changes and associated rights and must be kept at the company's principal office. Companies are required to keep trade books (TCC, art. 64), including those identifying shareholders and managers, in a complete, accurate and timely manner (TCC art. 65). These obligations are supported by sanctions. Companies that fail to maintain accurate trade books or update them as required are subject to administrative fines (TCC, art. 562) and potentially more severe penalties under the TPL. Corporate taxpayers in Türkiye must maintain accurate, adequate and up-to-date BO information under the Tax Procedure Law (Law No. 213) and Communiqué No. 529, filing quarterly with the TRA and reporting changes within one month. They must retain BO data for five years (art. 8(1) of the Communiqué; art. 253 of the Tax Procedure Law) and record shareholder and management details in the Trade Registry (Law No. 6102). This framework ensures that corporate taxpayers maintain current ownership and governance information accessible to competent authorities. The definition of beneficial owner is set out in the Regulation on Measures (RoM), Article 3(1)(h), and the measures for identifying the beneficial owners of legal persons are provided in Article 17/A. Accordingly, beneficial ownership information may be obtained from obliged entities that have business relationships with legal persons registered in the trade registry. Obliged entities are required to maintain up-to-date customer information, including beneficial ownership information, under ongoing monitoring obligations (RoM, Art. 19(1)), apply more frequent updates in higher-risk situations (RoM, Art. 26/A(1)(a); RoC, Art. 13(1)), and ensure that such information is kept current as part of monitoring and control activities (RoC, Art. 15(3)(e)).

b) Primary BO data is collected by the TRA, which operates the Beneficial Ownership Registry (Communiqué No. 529). This central registry is updated quarterly for corporate taxpayers and annually for others, with a one-month deadline for reporting any changes. BO information is also drawn from the Trade Registry and MERSIS, which store shareholding structures, company formation documents and changes in company management. This system enables competent authorities to access BO data efficiently without reliance on a single registry. Türkiye has documented its approach, which combines central reporting with decentralised recordkeeping. (ii) (***Not applicable***). (iii) Türkiye also relies on supplementary channels to support BO transparency, including: Information held by financial institutions (FIs) and certain designated non-financial businesses and professions (DNFBPs) obtained during customer due diligence under R. 10 and 22. Oversight is undertaken by the MKK for publicly traded companies while regulatory authorities and trade directorates monitor compliance, especially in co-operatives and other sectors.

Criterion 24.7

Türkiye has enforceable provisions requiring the retention of company and BO records for a minimum of five years. The TCC mandates that company books and records be kept for 10 years from the end of the calendar year in which the last entry was made (art. 82 (5)). This requirement applies broadly to all company types, including co-operatives (Co-operatives Law, art. 89) and covers books such as the share register, board decisions and accounting records. Obliged entities (such as FIs and DNFBPs) must retain transaction records, identification data and other related documentation for 8 years (AML Law, art. 8). Additionally, there is a requirement for taxpayers to keep all related documents (e.g., books, vouchers, contracts and declarations) for 5 years, beginning from the year following the transaction (Tax Procedure Law, art. 253–257). These retention periods apply to companies that are dissolved or otherwise cease to exist, as well as those that are former customers of a FI or professional intermediary (TPL, art. 164; AML Law No. 5549, TPL Communiqué No. 529).

Timely access to adequate, accurate and up-to-date information

Criterion 24.8

Mostly met) Türkiye employs multiple mechanisms to maintain accurate and up-to-date BO information, including databases like the Trade Gazette, MERSIS, the BO Registry and tax records, alongside information held by obliged entities and the CSD. Amendments to the TCC require the CSD to track bearer share ownership, and corporate taxpayers must update BO details quarterly, with changes reported within a month (Tax Procedure Law General Communique No. 529). The MASAK, in collaboration with tax inspectors and international exchanges, identifies inaccuracies and enforces corrections, supported by agreements with other agencies for enhanced oversight. Compliance inspections ensure BO obligations are met, and citizens can verify their BO status via the Interactive Tax Office, which provides an official QR-coded document for validation by obliged entities**.**

Adequacy Türkiye's framework ensures that all core elements of basic information, as defined by FATF, are collected, recorded and made publicly available through the Trade Registry, supported by clear legal obligations under the TCC (e.g. Arts. 31, 33, 35 and 354). The framework for collecting BO information includes detailed data requirements that largely align with FATF expectations. The only legal instrument that specifies the required data elements is Communiqué No. 529 on the Notification of Beneficial Ownership, issued under art. 148 and 149 of the Tax Procedure Law (Law No. 213). art. 7 of the Communiqué requires companies to complete a standardised "beneficial ownership information form," which contains four sections. This form collects identifying details of the legal person, identifies who qualifies as the beneficial owner and for each beneficial owner requires disclosure of the reason for inclusion (such as ownership of more than 25 percent, other control or senior executive authority). It also captures key identifiers including the person's name, address, date of birth, nationality (and any second nationality), job title, percentage and type of shares, the number of an identification or passport document, as well as details of the person authorised to submit the form on behalf of the company. These elements provide competent authorities with sufficient information to identify and trace the natural person who ultimately owns or controls a company and the mechanism through which control is exercised. However, it is not clear whether the "address" field in the form refers to a residential or business address and the guidance and form do not provide sufficient clarity. Associations, co-operatives and foundations that are tax exempt and small in number under Türkiye's law, provide basic information but do not maintain BO requirements. But detailed information on founders, members, donors, assets is maintained through DERBIS on associations. For foundations information with responsibility in executive organs of the foundations is maintained within the VBYS system. The Corporate Tax Law no 5520 (Art 2-4) does not exempt economic enterprises belonging to associations or foundations, and such economic enterprises are still required to file beneficial ownership information.

Accuracy (*Partly met*): The basic information submitted to MERSİS is subject to formal and procedural checks, with no explicit requirement to substantively verify the accuracy of the underlying information beyond document-based validation. Notarisation and supporting documentation provide a degree of formal validation, particularly in confirming the identity of individuals and the legal validity of submitted documents. However, these measures primarily ensure compliance with formal and procedural requirements and do not extend to substantive verification of the accuracy of the information. Türkiye's framework for ensuring the accuracy of BO information is largely based on self-declaration by reporting entities, with partial evidence of independent verification against reliable, independently sourced documents or data. Under the Tax Procedure Law (Law No. 213, art. 148–149) and Communiqué No. 529 on the Notification of Beneficial Ownership, corporate taxpayers are required to submit BO information to the TRA quarterly and to report any changes within one month. art. 8(1) of the Communiqué obliges taxpayers to retain BO information for five years, while art. 8(3) provides that where MASAK, tax inspectors or international information exchanges identify incorrect BO records, the GİB shall be informed to apply necessary sanctions and correct the data. These provisions establish a legal basis for collecting and amending BO information, but they do not create procedures for verifying the identity and status of beneficial owners using reliable, independent sources, as required by the FATF standard.

For BO information, there is reliance, primarily on self-reported data, supplemented by some cross-checking through MASAK's analytical functions, tax inspections and inter-agency protocols with the Tax Inspection Board and Ministry of Trade. There is no explicit requirement in Law No. 213, Communiqué No. 529, or related regulations for the Revenue Administration to verify BO submissions against independent databases such as population, passport or civil registries and limited information was provided on whether such sources are used in practice to support verification. Nor is there a clearly defined process for obliged entities' customer due diligence discrepancy reporting data to be systematically reconciled with the BO Registry. Although citizens and taxpayers may check BO declarations through the Interactive Tax Office and obliged entities may compare these against their records, this process is voluntary and there is limited information on the extent to which they are used to support verification in practice. As a result, while Türkiye's framework allows for the detection and correction of inaccuracies once identified, it does not demonstrate the existence of clearly defined and articulated processes for the independent verification of beneficial ownership information or that complementary measures effectively ensure the accuracy of data held in the BO Registry.

Up to date: There are clear legal requirements under the TCC for companies to ensure that basic information is kept updated. In particular, Article 31 requires that any changes to registered matters are also registered, supported by enforcement measures under Article 33. Additional provisions require the timely registration and announcement of specific changes, such as changes in shareholder structure (Arts. 338 and 574) and transfers of shares (Art. 598), while companies are also required to maintain updated shareholder registers (Arts. 499 and 594). These obligations are reinforced by the public nature of the Trade Registry (Art. 35) and the general requirement that records be maintained in a complete, accurate and timely manner (Art. 65), providing a framework to support the updating of basic information.

The legal framework establishes clear mechanisms for updating BO data. Under Communiqué No. 529 on the Notification of Beneficial Ownership, issued pursuant to art. 148 and 149 of the Tax Procedure Law (Law No. 213), corporate taxpayers are required to file BO information quarterly with their temporary tax returns and report any change within one month. This one-month update requirement aligns with the FATF expectation that BO information be updated "within a reasonable period following any change." Art. 8(3) of the Communiqué also allows for corrections when MASAK, tax inspectors or international exchanges identify inaccurate or outdated information. The quarterly and one-month reporting obligations apply only to corporate taxpayers; small tax-exempt co-operatives, associations and foundations are outside the regime and have no obligation to update ownership data but do have requirements to update changes in detailed basic and structural information that addresses this gap and is reflected in KOOPBIS, VBYS and

DERBIs. Economic enterprises created under such tax-exempt co-operatives are required to report beneficial ownership information. The framework utilises formal validation for basic information and relies predominantly on self-declared beneficial ownership information, with no clear requirement for systematic independent verification against reliable sources, which limits assurance of accuracy and up to date nature of information.

Criterion 24.9

Türkiye ensures that competent authorities, particularly LEAs and the FIU, have timely access to basic and BO information held by public authorities, FIs, DNFBPs and other relevant sources. Public prosecutors have broad investigative powers to obtain information from any public official or institution, including LEAs, MASAK, the Revenue Administration and the Ministry of Trade and can request any necessary information, including BO information and officials need to respond, "without any delay" (CPC art. 161). LEAs act under the direction of prosecutors and are similarly authorised to gather all necessary BO and company data. MASAK has direct access to the central BO Registry maintained by the Revenue Administration. Furthermore, MASAK can request any type of information from all natural and legal persons, access data processing systems of public agencies, including those holding financial, tax and company records, and obtain BO and shareholder data from multiple sources, including company registries and tax files (AML Law, art. 7 and 9). Tax Procedure Law General Communique No. 529 also requires all corporate taxpayers to file the BO information with their temporary tax returns (every 3 months) and if there is any change in the information, such change will be reported within one month.

The Revenue Administration is empowered by the TPL to collect BO information. Taxpayers and relevant persons are required to provide information upon request (TPL, art. 148). There is a requirement to report periodically (TPL, art. 149) and facilitate international exchange of information on request or spontaneously (TPL, art. 152 (A). The MERSIS contains basic company information and is publicly accessible. This allows authorities to confirm company legal status and identify persons authorised to act on the company's behalf (TCC, art.370 and 371). There is also the ability to obtain background on corporate structure and directors.

Regarding responsiveness, the Revenue Administration promptly responds to prosecutor or LEA requests. MASAK's 2021 Information Exchange as well as Co-operation and Co-ordination Protocols with the Ministry of Trade and Tax Inspection Board, respectively, further streamline access and co-ordination. No information was provided by the jurisdiction to demonstrate that public authorities, or other relevant bodies involved in public procurement, have timely access to basic and BO information for entities participating in procurement processes. It is therefore unclear whether such information is systematically used to verify the identity, ownership or control of legal persons in the course of awarding public contracts. MASAK and LEAs have clear and strong measures to obtain basic and BO information and to some extent, all applicable competent authorities across all legal persons can obtain basic information from the MERSIS system and BO information within ten days of written request (Criminal Procedure Law, art. 332) but no information was provided on timely access to BO information for non-law enforcement competent authorities.

Criterion 24.10

Türkiye utilises the BO Registry, other registries, and CDD information held by obliged entities to obtain basic and BO information for foreign-created legal persons and other legal persons with sufficient links.

Under Communiqué No. 529 issued by the Revenue Administration, foreign-created legal entities that have a main office or manager residing in Türkiye, or that are otherwise active in the country and fall within the scope of taxpayer obligations, are required to file BO information. This requirement extends to trusts and similar arrangements with an effective presence in Türkiye, companies conducting business and subject to taxation as limited taxpayers, and structures where foreign ownership exceeds 50% shareholding.

The framework provides mechanisms to ensure that BO data remains accurate and up to date. Where discrepancies are identified during MASAK inquiries, tax inspections, or through international information exchange, these findings are reported to the Revenue Administration. The Administration may then update the records and apply sanctions where necessary (Communiqué No. 529, art. 8(3)).

Competent authorities have access to basic legal entity information through multiple administrative registries. Information on companies and partnerships is maintained in the MERSİS system (Ministry of Trade, TCC, arts. 40–45), while co-operatives, associations and foundations are recorded in KOOPBİS (Law No. 1163), DERBİS (Law No. 5253), and the Vakıf Bilgi Sistemi (Law No. 5737), respectively. These systems provide direct access to essential data such as registration details, addresses and management information

The framework for ensuring the accuracy and up-to-datedness of BO information remains uneven. For BO data, the system relies predominantly on self-declaration by reporting entities, with no explicit requirement in the Tax Procedure Law, Communiqué No. 529 or related regulations for systematic verification against reliable, independently sourced data (e.g. population, civil or passport registries). There is a discrepancy reporting mechanism, for obliged entities to report inconsistencies between BO registry data and information held by obliged entities While cross-checking may occur through MASAK's analytical functions, tax inspections and inter-agency co-operation, these are ad hoc and not embedded within clearly defined, systematic verification processes.

For other legal persons—particularly associations and foundations recorded in DERBİS and VBYS—there is comparatively stronger monitoring of basic information, including structured reporting obligations and ongoing oversight by competent authorities, which contributes to a higher degree of accuracy of basic data.

The legal framework includes mechanisms to keep BO information up to date, reflecting a structured approach to maintaining current data. The quarterly reporting and one-month update requirements applicable to corporate taxpayers provide a clear and timely updating framework. While certain entities—such as tax-exempt co-operatives, associations and foundations—are not subject to BO reporting obligations, they are nonetheless subject to robust requirements to maintain and update basic and structural information through systems such as KOOPBİS, DERBİS and VBYS, which supports the overall reliability of legal person information. In addition, economic enterprises established by these entities remain within the scope of BO reporting obligations, ensuring that ownership information is captured where such entities engage in economic activity.

However, gaps in the mechanisms to ensure the accuracy of BO information, particularly the reliance on self-declared data and the absence of systematic independent verification—may in turn affect the extent to which BO information remains fully up to date in practice.

Criterion 24.11

Türkiye ensures timely access to public company information by FIs, DNFBPs and competent authorities of other countries, through a combination of digital and publicly accessible registries. Türkiye's Trade Registry (accessible at www.ticaretsicil.gov.tr) provides free, online access to key information on registered legal entities. Additionally, the MERSIS platform provides digital access to commercial registry transactions and associated corporate documentation.

Obstacles to transparency

Criterion 24.12

a) Türkiye has implemented legal and regulatory measures to prevent the misuse of bearer shares and ensure their traceability.

b) Türkiye does not prohibit the issuance of new bearer shares, but its legal framework effectively mitigates the associated risks by requiring dematerialisation and registration of all bearer shares (TCC, art. 488 (2)). Only joint stock companies are permitted to issue bearer shares. For listed joint stock companies, bearer shares are registered and monitored through the CSD in accordance with the Capital Market Law (CML, art. 486 and 489). For non-listed joint stock companies, all bearer shares are required to be reported to CSD before they are distributed to shareholders. Türkiye's laws do not recognise bearer share warrants.

c) Controls are in place for bearer shares issued by non-listed joint stock companies. Before issuance, the board's decision to issue bearer shares must be registered with the Trade Registry, published on the company's website, and the shareholder information reported to the CSD. Transfers of bearer shares must also be reported to the CSD, or the rights associated with those shares (e.g., voting, dividends) cannot be exercised (TCC, art. 486 and 489) and the issuance of printed shares that are registered must be done within three months of the payment of the share price. These measures effectively convert bearer shares into a registered and traceable form. Further, competent authorities have direct access to the MKK's records, ensuring timely access to ownership information.

Criterion 24.13

Türkiye has addressed the risk of misuse of nominee shareholding and nominee directorships by prohibiting such arrangements under its legal framework. Members of the Board of Directors cannot be represented by third parties during board meetings, thus preventing the use of nominee directors (TCC, art. 390 (2)). Shareholders may only act on their own behalf. Representation in general assembly meetings is only permitted through a formal power of attorney issued via notarial process and such representation is limited to specific corporate actions (e.g., voting) and does not amount to nominee ownership (Regulation on the Procedures and Principles of General Assembly Meetings of Joint Stock Companies and the Ministry of Representatives to be present at these Meetings, art. 18).

Liability and sanctions

Criterion 24.14

Obligations and sanctions applicable to R. 24 are distributed across company law, tax law and AML/CFT frameworks, creating multiple entry points for enforcement. There is a clear linkage between preventive obligations (e.g., BO disclosure, registry filings, CDD) and sanctioning provisions, supported by mechanisms such as automatic fine escalation, repeat-offence penalties and minimum threshold for CDD violations for certain financial institutions.

Sanctions are triggered primarily by failures to comply with registration, reporting and disclosure obligations, including BO reporting under the Tax Procedure Law, CDD obligations under AML/CFT rule, and corporate obligations under the TCC. These are complemented by administrative penalties for non-compliance across sectoral systems (e.g., DERBIS, VBYS), and by criminal sanctions for specific misconduct such as front person arrangements. The framework also includes non-monetary measures, such as suspension of shareholder rights (e.g., for bearer shares), strike-off of inactive companies, and dissolution powers under Article 210/3 of the TCC. There is an escalating penalty structure for repeated violations, notably for breaches. Sanctions for breaches of BO obligations are imposed under the Tax Procedure Law through an administrative fine framework with a built-in escalation mechanism for repeat violations. Under Article 355/bis, fines are automatically increased (tripled from the base amount) and further raised by 25% for repeated violations within a two-year period. Sanctions for CDD breaches under the AML/CFT framework are imposed primarily through administrative fines applied on a per-breach basis through fixed statutory amounts, with transaction-based minimum thresholds applying only to certain financial

institutions and not DNFPBs. This may not be sufficient for more serious ML/TF cases, especially when misconduct is willful or knowing.

Non-monetary administrative measures—such as suspension, deregistration or disqualification—are available to competent authorities. In most cases, the imposition of such measures requires a court order, including to effect changes in the trade registry, which limits the speed and flexibility of enforcement. Criminal liability cannot be imposed directly on legal persons under Turkish law; instead, sanctions against legal persons are primarily administrative in nature. In more serious ML/TF cases and cases involving larger legal persons, this can limit the dissuasive effect of the applied sanctions.

Bearer shares are not prohibited, but Türkiye mitigates the associated risks by requiring their dematerialisation and registration through the Central Securities Depository. Additional controls, such as the suspension of all shareholder rights — including dividend entitlements and general assembly participation — pending Central Securities Depository notification, provides a useful deterrent against non-registration. Penalties applied for non-registration of bearer shares are not fully dissuasive.

Overall, Türkiye's sanctioning framework has good variety, proportionality and dissuasiveness to address non-compliance across the spectrum of legal persons. Gaps remain in the sanctioning framework for CDD breaches and bearer share non-compliance. Although non-monetary administrative measures are available, their reliance on court orders—particularly for changes to the trade registry—limits the speed and flexibility of enforcement. Also, as criminal liability cannot be imposed on legal persons in Türkiye, the framework relies primarily on administrative sanctions, which may not be fully dissuasive for larger legal entities or in more complex ML/TF cases.

International co-operation

Criterion 24.15

Türkiye has established a multi-agency framework for international co-operation on basic and BO information, involving MASAK, the TRA, the MOJ and the MoT. This structure is supported by legal powers, operational tools and participation in international agreements and networks.

a) Türkiye's framework avoids undue restrictions on information exchange. MASAK adheres to the Egmont Principles which prohibit unreasonable limitations (e.g. based on tax secrecy or the nature of the request). Formal requests processed via the Law No. 6706 on International Judicial Co-operation in Criminal Matters (IJCL) are only rejected under limited grounds, such as threats to sovereignty or fundamental human rights violations, in line with international norms. Further, mutual legal assistance (MLA) is facilitated under multiple bilateral and multilateral treaties.

b) The Trade Registry Gazette and MERSIS provide public, online access to corporate information. MASAK, RA and MoT respond to foreign requests for basic and BO information, either directly or via formal co-operation channels, including diplomatic routes and MLA.

c) Shareholder data (including bearer shares) is accessible via MERSIS and the CSD (TCC, art. 486 and 489). MASAK, MoT and RA are empowered to exchange such information upon request.

d) MASAK, as the FIU and principal authority for AML/CFT, can access the BO Registry, tax databases and records from obliged entities and other government bodies. MASAK is authorised by PD No. 1 (art. 231) to conduct inquiries, including for foreign FIUs.

e) The MASAK established its April 2025 Guidelines on International Exchange of Information, which requires staff to complete feedback forms assessing responses received from foreign FIUs, including the quality of BO data. Feedback is used to monitor effectiveness and may be relayed to counterpart FIUs.

f) BO information is stored in the BO Registry (administered by the RA), MERSIS and obliged entities. MASAK has direct or indirect access to all major sources of BO information and can cross-check them for discrepancies to ensure accuracy.

g) Türkiye has clearly designated agencies based on the type of request, namely, the MASAK (BO and AML/CFT-related requests), the Revenue Administration (fiscal/tax matters under OECD and bilateral agreements), MoJ (MLA and criminal matters) and MoT (registry-related inquiries). Each agency operates within a well-defined mandate and engages with international partners using appropriate legal and operational tools (e.g., Egmont Secure Web, MLA channels, tax treaties).

Weighting and conclusion – Türkiye has developed a comprehensive framework for transparency of legal persons, supported by extensive registration systems (MERSİS, DERBİS, KOOPBİS, Vakıf Bilgi Sistemi) and clear statutory requirements for company formation, recordkeeping and governance. The establishment of a central Beneficial Ownership (BO) Registry under Communiqué No. 529 and the requirement for income and corporate taxpayers to update BO data quarterly and within one month of any change have strengthened oversight. However, gaps remain. Accuracy controls are largely self-declaratory, with basic company information subject only to formal checks, which contributes to verification to a limited extent and no clear requirement for substantive verification. Verification for beneficial ownership is ad-hoc, not risk-based and lacks clearly defined processes. The 2025 Legal Persons Risk Assessment builds on an existing data-driven foundation and reflects further efforts to refine and enhance the analytical framework. It would, however, benefit from further development in its treatment of foreign legal entities and related complex cross-border ownership structures and greater distinction in the analysis of TF risks between foreign and domestic legal persons. While Türkiye has effective mechanisms for bearer share control, nominee prohibition and international co-operation, minor deficiencies remain in the adequacy and accuracy of BO information, the coverage of risk assessment and its sanctions regime. **Recommendation 24 is rated largely compliant.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements[84]

In its 2019 MER, Türkiye was rated partially compliant with R.25 and through the follow-up process in 2022, was re-rated largely compliant. Minor shortcomings include the conclusion that sanctions for failure to perform AML/CFT obligations are still not dissuasive and there is no direct obligation on professional trustees to provide timely information to competent authorities, although trustees may be liable for failing to provide beneficial ownership (BO) information to an obliged party (such as lawyers).Türkiye is being assessed following changes to R. 25 which now require countries to: assess the ML/TF risks of misuse of legal arrangements, provide adequate, accurate, and up-to-date information on express trusts and other similar legal arrangements, ensure efficient and timely access to information by competent authorities and ensure that there is international co-operation between countries on express trusts and other similar legal arrangements.

[84] Recommendation 25 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

Scope extends to express trusts and other similar arrangements

Criterion 25.1

Türkiye is not a party to the Hague Convention on Trusts, does not permit the formation of domestic trust arrangements and has no legal arrangements equivalent to fiducie, Treuhand, or fideicomiso. Furthermore, Turkish foundations are treated as legal persons and do not resemble trusts, a conclusion supported by a dedicated risk assessment (Legal Person Risk Analysis, Chapter 2), which found no domestic equivalents or substitutes to trusts. Türkiye has, nevertheless, adopted legislative and regulatory measures to address the requirements of R. 25, including that trustees are to disclose the existence of a trust when initiating transactions with obliged entities in Türkiye and ensuring that obliged entities conduct customer due diligence (CDD), (RoM, art. 6, 7, 11(2) and 11(3)).

Criterion 25.2

Turkish law does not permit express trusts or other similar legal arrangements (c.25.1 refers).

Risk assessment and risk mitigation

Criterion 25.3

Although Türkiye is a non-trust law country and does not recognise or permit the establishment of domestic express trusts, the jurisdiction has conducted an assessment to evaluate potential exposure to foreign trust arrangements and to identify any equivalent domestic structures. The risk assessment takes a narrow view of legal arrangements, focusing mainly on those with a direct and visible presence in Türkiye. It does not fully capture risks from foreign legal arrangements with sufficient links that may be used indirectly or form a part of complex ownership structures, limiting its ability to reflect the full scope of ML/TF exposure.

a) There are no trusts governed under Türkiye's legal framework, thus c.25.3(a) is not applicable.
b) A risk assessment of foreign law trusts for which the trustee or equivalent resides in the country (c.25.3(b)) and foreign legal arrangements that have sufficient links with Türkiye (c.25.3(c)) has been completed. See IO.5 for more information (Basic and Beneficial ownership information).
c) The risk assessment considers legal arrangements and their nexus to Türkiye through a relatively narrow aperture, focusing primarily on situations where the legal arrangement has a direct and visible presence or interaction with the jurisdiction. However, legal arrangements may also form part of multi-layered ownership or control chains of legal persons operating in Türkiye. The increased exposure arising from the indirect use of legal arrangements within ownership structures is not fully captured, which limits the assessment's ability to reflect the full range of associated ML/TF risks.

Basic and Beneficial ownership information

Criterion 25.4

Türkiye is a non-trust law country and non-party to the Hague Convention on Trusts but it has introduced legal, regulatory and supervisory measures to address the risks associated with foreign trust agreements administered or connected to Türkiye, particularly where the trustee resides in or transacts within the jurisdiction.

a) Türkiye requires that when a trustee of a foreign trust requests a transaction, they must disclose in writing, to the obliged entity, the nature of the trust relationship prior to the transaction. The trustee

must also provide copies of the trust deed and customer identification information, verified through notarised Turkish translations using a risk-based approach. The obligation extends to carrying out reasonable measures to verify identity information of the settlor(s), trustee(s), protector(s), beneficiaries or class of beneficiaries, Necessary measures shall be taken for revealing the identity of the person with effective control and any other person with ultimate effective control. (RoM, art. 11(2) and (3).

b) Obliged entities are required to identify and verify beneficial ownership (BO) information, not only for individuals, but also for any legal persons involved in the trust. This includes necessary measures to identify the natural persons (RoM, Art. 11 (2)) who ultimately control the trust's assets. These requirements are supported by the BO Registry, established under the Tax Procedure Law (TPL) General Communique No. 529 (2021). Additionally, MASAK has produced Guidance on the Obligation on Identification of Parties to a Trust Agreement Established Abroad (2021).

c) Lawyers, accountants and other agents are covered as obliged entities (RoM, art. 4(1)). These professionals are subject to the same CDD and BO obligations when involved in transactions related to foreign trusts. MASAK's supervisory findings indicate no evidence that these professionals are acting as trustees, but AML/CFT obligations are imposed on them, should instances be identified. Furthermore, the BO Registry is operated by the Revenue Administration in co-operation with MASAK. The BO Registry requires corporate taxpayers and trust managers/trustees of foreign legal arrangements with a presence in Türkiye to submit BO information quarterly or annually. It also requires that any change must be reported within one month. The BO Registry also maintains information for five years and imposes sanctions for non-compliance, including incomplete or misleading submissions. The BO form to be completed includes the identification of the legal person/legal arrangement, criteria for BO classification (ownership, control, trustee, settlor, beneficiary etc.), detailed BO information (name, nationality, date of birth, identification, share %, role) and the filing party's contact information and signature.

Criterion 25.5

Türkiye is not a party to the Hague Convention on Trusts and its domestic legislative framework does not permit the establishment of express trusts or similar legal arrangements. Nevertheless, Türkiye has taken appropriate measures to ensure that, should trustees or persons holding equivalent positions in similar legal arrangements operate within its jurisdiction, they are subject to robust recordkeeping obligations concerning BO information.

There is a legal requirement for trustees of foreign trusts to disclose their status and provide identification documentation and trust deeds to obliged entities prior to engaging in transactions (RoM, art. 11(2) and 11(3)). Obliged entities, which include lawyers and accountants (those most likely to act as trustees) are subject to the record-keeping requirement under the AML Law (art. 8), which mandates that all transaction records, CDD information and supporting documentation be retained for eight years from the date of creation or final transaction. Additionally, all corporate taxpayers—including foreign trust managers or representatives with a presence in Türkiye—are required to report BO information under the Tax Procedure Law Communique No. 529 and retain this information for five years (Communique No. 529, art. 8(1). Furthermore, there is an obligation on all taxpayers to retain records related to books and documents for five years after the close of the fiscal year to which they relate (TPL, art. 253). Although no trustees or equivalent persons are currently operating in Türkiye, these legal obligations ensure compliance with the FATF requirements.

Criterion 25.6

Türkiye has established a legal and regulatory framework that requires BO information held pursuant to c. 25.4 to be accurate, up-to-date and subject to timely updating following any changes. The BO Registry, implemented through the TPL General Communique No. 529, mandates that corporate taxpayers must file

BO information quarterly with their temporary tax returns. Other taxpayers must submit BO information annually by the end of August. In cases of change, updated BO information must be filed within one month of the change. This requirement applies explicitly to trustees or representatives of trusts and similar legal arrangements that have a main office or managerial presence in Türkiye.

Additionally, the AML/CFT regime reinforces ongoing accuracy through continuous monitoring obligations imposed on obliged entities. More particularly, obliged entities must monitor customer transactions and profiles to ensure that information, including BO details, remains current (RoM, art. 19(1)). There is also a requirement for enhanced due diligence measures, including more frequent updates of BO information, particularly for higher-risk customers (RoM art. 26/A(1)(a)). Similarly, obliged entities must adopt risk-based updating procedures to address BO risks more frequently for high-risk customer segments (Regulation on Compliance (ROC, art. 13(1)). There is also an obligation for internal control functions to verify that BO and other customer data remain up to date as part of ongoing monitoring (RoC, art. 15(3)(e) and 32/A).

These requirements are binding on all obliged entities, including lawyers and accountants, who are the professionals most likely to interact with trust arrangements. As such, Türkiye ensures that parties with potential access to or involvement in trust-like arrangements are obligated to maintain and update BO data in a timely and risk-based manner.

Criterion 25.7

Although Türkiye does not recognise or permit the formation of domestic trusts and is not a party to the Hague Convention, it has implemented a legal and regulatory framework that ensures trustees of foreign trusts and persons in equivalent roles in similar legal arrangements are subject to key obligations. There are no significant restrictions that impede the provision of information to competent authorities.

a) Türkiye requires any trustee of a foreign trust who seeks to engage with a FI or DNFBP to disclose their status in writing prior to conducting a transaction or establishing a business relationship (RoM), art. 11(2)). This obligation applies broadly to trustees acting on behalf of trust arrangements established abroad. Conditions and thresholds have also been established for when customer identification is required, including when forming a business relationship or conducting transactions above defined monetary limits (RoM art. 5). Further, there is a requirement on obliged entities to identify individuals acting on behalf of or for the benefit of others, with public notice requirements reinforcing the obligation to self-declare such relationships (RoM, art. 14 and 17). Failure to declare that a transaction is carried out on behalf of another person (e.g., as a trustee) constitutes an offence punishable by imprisonment or a fine (AML Law, art. 15).

b) Türkiye has established a legal basis to ensure that trustees are not prevented from co-operating with competent authorities. There is an obligation on all public and private entities, including natural and legal persons, to fully and accurately provide all requested information, documents and records to MASAK or other designated examiners upon request (AML Law, art. 7). Claims of confidentiality under special laws cannot be invoked, except where legal defence rights apply. Additionally, prosecutors are empowered to request information from FIs, DNFBPs and public institutions (Criminal Procedure Law, art. 161(1)).

c) There are laws that govern trustee interactions with obliged entities, requiring trustees to provide full disclosure of the trust relationship, BO information, documentation on any assets held or managed under the trust agreement (RoM, art. 11(2)). There is also a mandate that customer identification must be completed prior to the establishment of a business relationship or execution of a transaction, with no exemptions for trustees or other customer types (RoM art. 5(2)). Consequently, if a trustee does not provide the required information, the obliged entity is legally prohibited from proceeding.

Timely access to adequate, accurate and up-to-date information

Criterion 25.8

Türkiye has established mechanisms to ensure that information collection on trusts and similar legal arrangements. There are however minor deficiencies in the law (RoM, art 11(2)) that prevent adequate information on trusts from being captured and the absence of a systematic comprehensive risk-based verification mechanism that limit the accuracy and up to date nature of information.

Adequacy of information: Türkiye's Regulation on Measures (RoM) provides a framework for identifying and verifying the parties to a foreign trust, however there are gaps which limit its ability to fully meet the FATF standard on verification. The provision states that "where necessary, customer identification information shall be verified through notarised Turkish translations of these documents within the risk-based approach" which introduces appropriate discretionary language ("where necessary"). However, the obligation on identification of parties to a trust agreement established abroad does not provide sufficient illustrative guidance on when it is appropriate to carry out verification. As trusts and similar legal arrangements do not exist under Turkish law and there is little operation in practices, obliged persons generally have limited experience in assessing and managing risks associated with such structures. In practice, this could result in inconsistent application across FIs, particularly where foreign documents are relied upon.

The text requires obliged entities to take reasonable measures to verify identity information for the settlor, beneficiaries and protector, but it does not specify the minimum documentation or verification methods to be used. The reference to "reasonable measures" leaves the quality and depth of verification open to interpretation, potentially leading to reliance on unverified foreign documents or self-declarations. The phrase "necessary measures shall also be taken for revealing the natural person(s) who ultimately control(s) the mentioned assets" further weakens the provision. The term "revealing" implies discovery or identification, but not formal verification through independent, reliable sources as required by the FATF Standards. The Guidance on Obligation on identification of parties to a trust agreement established abroad does not contain guidelines to demonstrate that this is treated as verification.

Up to date information: Updated BO information must be submitted within one month of any change. The data must be retained for five years and is subject to sanctions for non-compliance, missing or misleading information. Gaps in measures related to accuracy of information, impact accuracy and the up-to-date nature of information.

Accuracy of information: The BO Registry, created by the TPL is a central mechanism for capturing and verifying BO information related to legal persons and legal arrangements, including trustees or representatives of foreign trusts with a management presence in Türkiye. Key features include the requirement for corporate taxpayers to file BO information quarterly while other taxpayers file annually. Updated BO information must be submitted within one month of any change. The data must be retained for five years and is subject to sanctions for non-compliance, missing or misleading information.

To ensure accuracy and completeness, Türkiye has ad hoc established a cross-checking mechanism through analysis, inspections and information sharing. MASAK may identify discrepancies through domestic analysis, international information exchange or feedback from tax inspections and such discrepancies are reported to the Revenue Administration for correction and sanctioning. Interagency protocols are also in place (e.g., among MASAK, the Tax Inspection Board and the Ministry of Trade) to enhance information exchange and quality control. Türkiye has also introduced public-facing validation measures, for instance, individuals can log into the Interactive Tax Office to verify whether they are recorded as a beneficial owner. This e-verification tool can be used by obliged entities (e.g., FIs or DNFBPs) as an additional verification method when dealing with foreign trust customers. Furthermore, supervisors assessing AML/CFT compliance are tasked with verifying the accuracy and currency of BO information provided by obliged

entities, especially in relation to trustees of foreign trust agreements (RoM, art. 35). However, while mechanisms exist—such as updates under Communiqué No. 529 (Article 8 of the Tax Procedure Law) based on MASAK reports, tax inspections, and international information exchange, as well as interagency protocols among MASAK, the Tax Inspection Board, and the Ministry of Trade—their largely ad hoc application and the absence of clear requirements and defined processes limit the extent to which the framework ensures the accuracy.

Criterion 25.9

Türkiye has established a multi-source, risk-based framework to ensure that competent authorities can efficiently and in a timely manner access adequate, accurate and up-to-date information on basic and BO of trusts and similar legal arrangements, without relying solely on trustees. This is achieved through legal obligations, a central registry, interagency access and regulated gatekeepers.

a) Türkiye maintains a central BO Registry, established via a 2021 Tax Procedure Law General Communique and which is jointly administered by MASAK and the Revenue Administration. The registry requires quarterly BO filings from corporate taxpayers and annual filings from others; covers trustees or representatives of foreign trusts or similar arrangements with a management presence in Türkiye; requires updates to BO information within one month of changes; provides comprehensive identity and control information on beneficial owners; is enforceable with sanctions for non-submission or inaccurate filings; and ensures that Türkiye has a central, authoritative source for BO data that is both accessible and regularly updated.

b) Other competent authorities that maintain or can obtain trust-related information include the MASAK which has direct access to the BO Registry and to complementary databases, including tax records, commercial registries, suspicious transaction reports (STRs) and customs data. This access allows MASAK to verify BO information and identify trust-held assets. Prosecutors are empowered to request any relevant information from public institutions or officials during the course of an investigation (Criminal Procedure Law, art. 161(1)). These mechanisms ensure that competent authorities can obtain both BO and asset-related data without having to rely solely on trustees or similar parties.

c) Lawyers and accountants—the professionals most likely to interact with trust arrangements—are designated obliged entities under the AML/CFT regime and are required to maintain customer and BO records, provide such information to MASAK or other competent authorities upon request (AML Law, art. 7(1)) and comply with customer due diligence (CDD) and record-keeping obligations that include trust-related roles and assets (RoM, art. 11, 19, 26/A and 31). Additionally, all FIs and DNFBPs must conduct CDD, monitor client relationships and disclose BO information during supervisory checks.

Criterion 25.10

Türkiye has established a strong legal and institutional framework that ensures LEAs, MASAK and other competent authorities have the necessary powers to obtain timely access to information related to trusts and similar legal arrangements. These powers extend to information held by trustees, equivalent persons, FIs and DNFBPs.

a) Competent authorities in Türkiye, particularly MASAK and public prosecutors, have wide-ranging powers to access BO information. MASAK is authorised to request any information from all natural and legal persons and directly access the BO Registry, as well as data held by public institutions, including economic, tax and financial activity records (AML Law, art. 7 and 9). Public prosecutors and LEAs are empowered to request and obtain any kind of information from FIs, DNFBPs, public institutions and private persons. They can also require that such information be provided "without any delay" (Criminal Procedure Law, art. 161(1) and (4)). Regarding tax matters, there is an obligation on taxpayers and entities to provide BO information to the Ministry of Treasury and

Finance and the Revenue Administration, for international exchange and routine supervisory access (Tax Procedure Law, art. 148, 149, and 152/A).

b) LEAs, under the authority of public prosecutors, may conduct searches and obtain location data as part of criminal investigations. Türkiye maintains a centralised resident address system administered by the Ministry of Interior, known as the ID Sharing System. LEAs under the Ministry of Interior have direct access to this system, enabling the identification of residences of trustees or equivalent persons without delay.

c) MASAK has the authority to access financial and transactional data held by FIs and DNFBPs, including information on assets held or managed by these institutions on behalf of trustees. These powers are exercised during ML/TF risk analyses. Further, prosecutors and LEAs can also request information on assets held by or linked to trustees or their equivalents. (Criminal Procedure Law, art. 161).

Liability and sanctions

Criterion 25.11

Türkiye has established a legal framework overall that assigns clear responsibilities, imposes liability and ensures the availability of effective and proportionate sanctions, for failures related to trust-related obligations, however minor gaps remain that prevent the sanctioning framework from being effective, proportionate and dissuasive.

a) Türkiye has clarified the responsibilities of both taxpayers and obliged entities (including FI and DNFBPs) through the Tax Procedure Law General Communique no 529 which outlines detailed BO reporting obligations, frequency and scope (e.g. trustees and representatives of foreign trusts with a management presence in Türkiye). CDD and disclosure obligations are also imposed on obliged entities interacting with foreign trusts (RoM, art. 11, 17 and 17/A). The BO reporting and CDD framework are also captured under the AML and Tax Procedure Laws (TPL).

b) Trustees or equivalent persons, where they exist, are subject to liability and sanctions under multiple instruments. Taxpayers (including trustees) must comply with BO reporting rules (TPL, art. 355). Fines for non-compliance are three times the standard special irregularity fine, now up to TRY 84,000 (approx. EUR 2 304). Repeat violations within two years trigger a 25% increase in fines (TPL, art. 339). Obliged entities, including FIs and DNFBPs, face administrative fines if they: fail to perform CDD related to trust relationships, do not identify the BOs of a trust and fail to determine whether a client is acting on behalf of another. The legal design under Article 13 of the AML law—where fines are largely imposed on a per-breach basis using fixed statutory amounts, and transaction-based minimum thresholds apply only to certain financial institutions (excluding DNFPBs)—limits the ability of penalties to reflect the overall seriousness and scale of violations. As criminal liability does not apply to legal persons under Turkish law, and only administrative sanctions are available; in more complex ML/TF cases involving a legal person as trustee, the sanctioning framework is not fully effective, proportionate and dissuasive.

   Criminal penalties only apply, namely, imprisonment (6 months–1 year) or a judicial fine of up to 5,000 days when there is a failure to declare a transaction carried out for the benefit of a foreign trust (AML Law, art. 15)

c) Access to information by competent authorities must be timely and Türkiye has established offences and sanctions for obstruction or non-compliance. All public and private entities are obliged to provide requested information to MASAK and other authorities (AML Law, art. 7). There is also a requirement for public officials to comply without delay with requests made by public prosecutors (Criminal Procedure Law No., art. 161(4)). Further, it is an offence for entities to fail to declare that a transaction is made on behalf of a trust (AML Law, art. 15).

International co-operation

Criterion 25.12

Türkiye has comprehensive legal, institutional and operational frameworks to provide international co-operation in relation to trusts and other similar legal arrangements, particularly regarding BO information on the bases set out in R. 37 and R. 40.

a) Türkiye does not impose undue restrictions on international co-operation and exchange of BO information. MASAK exchanges BO data via both bilateral MoUs and the Egmont Secure Web, in line with Egmont Principle 24, which prohibits unreasonable barriers to information exchange. Türkiye also abides by applicable bilateral/multilateral legal assistance treaties and may only refuse requests on grounds consistent with international standards (e.g., sovereignty, human rights protections) (Law No. 6706 on International Judicial Co-operation in Criminal Matters (LIJCCM), art. 4). These provisions are also reflected in Target 1.2 of Türkiye's AML/CFT Strategy (2021/16), which prioritises enhanced international co-operation.

b) MASAK, the Revenue Administration (tax matters) and the Ministry of Justice (MLA) each provides access to BO and basic trust information to their respective foreign counterparts. These authorities act as central conduits and facilitate access to BO registries and asset records upon request.

c) Türkiye empowers its competent authorities (especially MASAK) to obtain and exchange domestically available trust-related information, including on trustees and legal arrangements. MASAK is authorised to conduct analysis, examination, search and supervision to gather such information for international exchange (PD No. 1, art. 231).

d) Competent authorities, particularly MASAK, are authorised to exercise their full domestic powers - including access to registries, tax records, and supervisory data- to respond to foreign BO information requests (PD No. 1, art. 231). The powers also include tracing and analytical functions.

e) MASAK is publicly designated as the central supervisory authority for BO information exchange on AML/CFT matters. In July 2021, MASAK issued an internal Guideline on Exchange of Information, updated in April 2025, which includes procedures for evaluating and tracking co-operation effectiveness. The Revenue Administration (for tax matters) and the MoJ (for judicial co-operation) are likewise designated as contact points for relevant BO information sharing. MASAK has access to the BO Registry and can exchange BO information via the Egmont Secure Web. Both MASAK and other competent authorities can exchange information via other secure channels (cc. 40.2 refers).

> ***Weighting and conclusion –*** Since its 2019 mutual evaluation Türkiye has worked to address the most significant gaps identified. Minor gaps continue to exist on the access to accurate and up to date information, the imposition of penalties and the analysis of all types of legal arrangements with sufficient links in the LPRA. Recommendation 25 is rated **largely compliant**.

Recommendation 26 – Regulation and supervision of financial institutions[85]

In its 2019 MER, Türkiye was rated partially compliant with R.26 and re-rated to compliant in its 2023 FUR.

Criterion 26.1

[85]This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019 and 2023 FUR, with minor non-substantive edits included from Türkiye.

MASAK regulates and supervises the AML/CFT obligations of FIs through different agencies. Supervision of the AML obligations is carried out through the examiners assigned to conduct supervision (AML Law, art.11): Tax Inspectors, Treasury and Finance Experts employed at MASAK, Customs and Trade Inspectors, Sworn-in Bank Auditors, Treasury Comptrollers, Insurance Supervisory Experts and Actuaries, Banking Regulation and Supervision Agency and Capital Markets Board Experts and Central Bank Auditors and Experts. Examiners who carry out AML/CFT supervision in the name of MASAK are personnel of BRSA, CMB, CBRT and MoTF as well as Ministry of Customs and Trade.

The BRSA is responsible for regulation and supervision of banks, factoring companies, financing companies, saving financing companies and leasing companies; and the CMB is responsible for regulation and supervision of capital market intermediaries and crypto asset service providers. Since October 2019, the MoTF General Directorate of Insurance has become a separate regulatory and supervisory authority named Insurance and Pension Regulation and Supervision Agency (IPRSA), responsible for the regulation and supervision of insurance and private pension companies. Regulation and supervision of Payment and E-money Institutions have been transferred from BRSA to the CBRT. Thus, they are now licensed by CBRT.

The GDFMFE supervises exchange offices.

In addition, MASAK may prepare a supervision program in co-operation with the related supervisory authority, and it has also authority to request the supervisory authority to include the supervision of obligations in its supervision program. The authority which is to conduct supervision of obligations has to fulfil this request (ROM, art. 35(4)).

Market Entry

Criterion 26.2

Core principles institutions and other FIs are required to be licensed in Türkiye. BRSA, CMB, IPRSA, CBRT and MoTF are licensing authorities for core principles FIs and other FIs. Though there is no explicit mention about debarring operations of 'shell bank' in Türkiye, the existing regulations do not leave scope for starting operation of shell bank in Türkiye. The following table sets out the licensing requirements in Türkiye:

Table A.2.Licensing requirements

Licensing Authority	FIs	Relevant Legislation
BRSA	Banks	Banking Law No.5411
	Financial leasing, factoring and financing and saving financing companies	Financial Leasing, Factoring and Financing and Saving Financing Companies Law No.6361
CBRT	Payment and e-money institutions	Law No.6493 on Payment and Security Settlements Systems, Payment Services and Electronic Money Institutions
CMB	Capital market institutions, intermediary institutions, portfolio management companies, real estate investment companies, securities investment companies, venture capital companies, Other capital market institutions	Capital Market Law No.6362 (CML)
	Crypto Asset Service Providers	Capital Market Law No.6362 (CML)
MoTF	Exchange offices	Communique No. 2018-32/45 attached to the Decree No. 32 Regarding the Protection of the Value of Turkish Currency
IPRSA	Insurance and reinsurance companies	Insurance Law No.5684
	Pension companies	Law No.4632 on Individual Pension Savings and Investment System

Criterion 26.3

Supervisory authorities (BRSA, CBRT, CMB, IPRSA and MoTF) have measures to prevent criminals and their associates from holding a significant or controlling interest, or a management function, in a FI, as it is required that founders, qualified shareholders and managers operating in senior roles have not been convicted of crimes including financial crimes. Requirements extend to those directly or indirectly exercising control in case of banks, insurance, capital market institutions, crypto asset service providers and other FIs. Supervisory authorities carry out fit and proper tests of FIs in the context of licensing requirements and procedure. In 2021, Türkiye amended the Communiqué concerning decree No. 32 on the Protection of the Value of Turkish Currency (Communiqué No: 2018 – 32/45)", the scope of fit & proper requirements in the establishment of exchange offices has been expanded to cover persons related to the legal person partner (art. 3/1(s),6/1(d), 6/2, 6.4, 7(b)). Therefore, in addition to natural person founding partners, any person with more than 10% share in the legal person founding partner, general manager of the exchange office, member of board of directors, employees with signatory authority and internal control officers, persons related to the legal person partner should also not have convictions (even if they were pardoned) for several crimes including extortion, bribery, theft, money laundering, terrorism financing (Article 6 (1)(d)(2)).The list of crimes were also expanded to include crimes listed in Law no.7262 on Prevention of Proliferation of Weapons of Mass Destruction. Additionally, if a share transfer take place, the natural persons who take over the shares have to meet the conditions sought for founding partners (art. 18 (2)).

Risk-based approach to supervision and monitoring

Criterion 26.4

(a) – (b) In 2020, MASAK prepared a Policy and Methodology document for Risk Based Supervision of Obligations, for FIs subject to core principles institutions and for all other FIs. The document sets forth the framework for risk-based supervision of obligations and determines the principles and procedures for an effective risk-based ML/TF supervision approach. According to the methodology, ML/TF risk analyses will be carried out every year by taking the National Risk Assessment into account and financial institutions will be categorised according to their risk scores. High risk financial institutions will be supervised every year and medium risk financial institutions every three years at the latest. For exchange offices, MASAK carried out a separate risk analysis in co-operation with General Directorate for Financial Markets and Foreign Exchange (GDFMFE) and Treasury Controllers Board (TCB). All this information indicates that Türkiye implement a RBA in supervising their FIs. The AML Law obliges the FIs to implement group-wide AML/CFT programs and obliges the Supervisory Authorities to ensure such prescribed measures are adopted by the supervised institutions under the supervision of such Authorities. With the amendments introduced in 2020 to AML Law, in 2021 to the RoC, and in conjunction with article 35 of RoM, MASAK has the authority to determine the extension and the scope of supervision under the discretion allowed by the risk base approach, both to FIs and financial groups for AML purposes.

Criterion 26.5

Since the publication of Policy and Methodology Document for Risk Based Supervision of Obligations in January 2020, Türkiye carried out comprehensive risk analysis activities and prepared a risk-based Supervision of Obligations Programs. The risk analyses not only determined and assessed the inherent risks in the sector but also evaluated the control measures applied by financial institutions to mitigate their risks. Furthermore, in addition to the residual risks, several other risk factors such as materiality; operational structure and diversity of offered products and services; training and internal audit reports prepared by financial institutions; information from MASAK database and supervisory authorities responsible for the sectors are also taken into consideration in the risk analyses. As a result of the risk analyses and in

accordance with the Methodology, financial institutions are categorised into three groups according to their risk levels (high, medium, low) and supervision programs are prepared accordingly.

According to the principles of Türkiye's supervision methodology which states that, ML/TF risk analyses will be carried out every year and financial institutions will be categorised according to their risk scores; high risk financial institutions will be supervised every year and medium risk financial institutions every three years at the latest.

It should also be noted significant weight was given to the supervision of high-risk sectors, as determined by Türkiye's NRA and MER. High risk sectors such as banks, exchange offices and payment and e-money institutions comprise more than 55% of the financial institutions supervised in 2022.

The intensity of risk-based supervision according to the Risks of Obliged Parties should also differentiate the intensity of risk-based supervisions according to the risks of obliged parties in both quantity and quality and according to the risks in the risk categories such as customer, product, service, country/geographical region, distribution channel, etc., of obliged parties.

Criterion 26.6

MASAK periodically reviews ML/TF risk profiles of obliged parties. Regulation on Compliance (RoC) covers articles related to taking measures commensurate with the risk. The scope of the compliance programs including risk management activities is reviewed and updated every two years based on risk perceptions (RoC, art. 5[1], 5[4]). MASAK supervises compliance of obliged parties with these obligations. Moreover, in line with the strategic objective II of AML/CFT strategy document, Türkiye updates its NRA and sectoral risks are further assessed. In this regard, the NRA action plan stipulates reviewing sectoral risks and prioritizing supervision activities based on risk perceptions. The Target III of the NRA Action Plan is about improvement of capacity for supervision and level of compliance and in this regard, activities 3.1, 3.2 and 3.4 are about updating risk-based supervision methodology and ensuring updating of compliance programmes to be prepared by obliged parties. Moreover, activity 3.5. is for all supervision units on prioritising controls in their fields based on ML/TF risks.

In this regard, other relevant agencies pay attention to ML/TF risk profiles of obliged parties. For example, BRSA periodically reviews the risk profiles of FIs under their supervision. BRSA has been assessing the compliance level of FIs as a part of its regular prudential and conduct of business supervision process. Hence, AML/CFT compliance level of the banks have been evaluated in an embedded process in the regular supervisions as part of CAMELS, covered under 'M', the management. With the increasing complexity of financial systems and the emergence of new risks, a more comprehensive and forward-looking supervisory approach was needed. In this context, the "Supervisory Review and Evaluation Process" (SREP) was established in November 2022 based on the Supervisory Review and Evaluation Process adopted by the European Banking Authority (EBA) instead of CAMELS. AML/CFT compliance level of the banks are evaluated in an embedded process in regular supervisions as part of SREP previously covered under "M" the management of CAMELS Methodology. With the transition to the SREP system, the weight of ML/TF/PF risks in the supervision processes have been increased and direct supervision points for the assessment of these risks have been added. Since 2020, Türkiye has put in place the Policy and Methodology Document for Risk Based Supervision of Obligations and has determined the principles and procedures for an effective risk-based ML/TF supervision approach. In line with the AML/CFT Strategy Document, NRA Action Plan and risk based supervision methodologies, ML/TF risk analyses are carried out every year and financial institutions are categorised according to their risk scores (Chap.4 (Principles of Risk Based Supervision Approach) and Chap.5 (Stages Concerning Risk Based Supervision Approach) of the policy and Methodology Document).

Weighting and conclusion – All criteria are met. Recommendation 26 is rated **compliant**.

Recommendation 27 – Powers of supervisors[86]

In its 2019 MER, Türkiye was rated largely compliant with R.27.

Criterion 27.1

MASAK, as the supervisory body, has the authority to ensure supervision of obligations within the scope of AML/CFT (PD 1, art.231(1)(i)). Supervision of the AML obligations is carried out through the examiners assigned to conduct supervision ((AML Law, art.11): Tax Inspectors, Treasury and Finance Experts employed at MASAK, Customs and Trade Inspectors, Sworn-in Bank Auditors, Treasury Comptrollers, Insurance Supervisory Experts and Actuaries, BRSA and the CMB experts and CBRT Auditors and Experts (AML Law, art. 2(1)(e). Examiners have powers to request all kind of information, documents and they can also use the powers given to them by other laws[87](ROM, art.36).

Criterion 27.2

MASAK has the authority to conduct inspections of FIs through the examiners assigned to conduct supervision as described under Criterion 27.1. In addition, obliged entities including FIs should provide all necessary facilities including to ensure proper working conditions (in their premises) for examiners during the process (ROM, art. 36(3)).

Criterion 27.3

When requested by MASAK or examiners, public institutions and organisations, natural and legal persons, and unincorporated organisations should fully and accurately provide all kinds of information, documents and related records any information or passwords necessary for accessing to or making these records decipherable, and render necessary convenience (AML Law, art.7).

Criterion 27.4

MASAK has the possibility to take sanction decisions and apply sanctions to FIs for failure to comply with AML/CFT requirements. The range of penalties and administrative sanctions include monetary penalty, judicial sanctions, license cancellations (AML Law, art. 13-14). See analysis under R. 35.

> ***Weighting and conclusion –*** All criteria are met, except for c.27.4, due to deficiencies identified under R.35.. Recommendation 27 is rated **largely compliant**.

Recommendation 28 – Regulation and supervision of DNFBPs[88]

In its 2019 MER, Türkiye was rated partially compliant with R.28 and re-rated largely compliant in its 2023 FUR.

Casinos

Criterion 28.1

Not applicable as casinos are not operating in Türkiye.

[86] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

[87] Such as Banking Law, Capital Market Law, Insurance Law, Tax Procedure Law.

[88] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019 and FUR 2023, with minor non-substantive edits included from Türkiye.

DNFBPs other than casinos

Criterion 28.2

MASAK is the competent authority for monitoring and ensuring the compliance of the DNFBPs operating in Türkiye with regard to the AML/CFT requirements (PD 1, art. 231(1)(i)).

Criterion 28.3

MASAK is the competent authority for monitoring and ensuring the compliance of the DNFBPs operating in Türkiye with regard to the AML/CFT requirements (PD 1, art. 231(1)(i)).

Criterion 28.4

a) MASAK's powers to monitor and ensure compliance are the same for FIs and DNFBPs. For details, see R.27.

b) Real estate agents, dealers of precious metals and stones, lawyers, notaries and accountants must apply to the relevant supervisory authority to have their officers and managers approved for undertaking their respective activities. In addition, if a person is sentenced to a penalty of imprisonment for an intentional offence, the person cannot be the administrator or inspector of a legal entity. Further, the offender cannot conduct any profession or trade, which is subject to the permission of a professional organisation, under his own responsibility as a professional or a tradesman (TCL No.5237, art. 53). Fit & proper requirements applied to these categories are: real estate agents (Regulation on Trade of Immovable, art.6); Dealers of precious metals and precious stones (Law No 5362, art. 6 and 7); Lawyers (Law No 1136, art. (3-10)), Notaries (Law No 1512, art. 7) and Accountants (Law No 3568, art. 4 and 5). These requirements do not extend to associates of criminals from being professionally accredited or holding (or being the beneficial owner of) a significant or controlling interest in a DNFBP.

c) Türkiye has sanctions available mostly in line with R.35 (rated LC) to deal with failure to comply with AML/CFT obligations by DNFBPs (AML Law, art. 13 –14) (also see R.35).

All DNFBPs

Criterion 28.5

a) MASAK developed sectorial risk assessments taking into account the diversity and the number of the sectors under DNFBP.

b) Starting from 2021, MASAK's supervision of DNFBPs is performed on a risk-sensitive basis, taking into account the risk profile of each sector and/or obliged entities. MASAK included DNFBPs in 2021 in the Policy and Methodology Document for Risk Based Supervision of Obligations of 2020. According to the methodology, ML/TF risk analyses will be carried out every year by taking the NRA into account and obliged parties will be categorised according to their risk scores. High risk obliged parties will be supervised every year and within the scope of available resources medium risk obliged parties every three years. In addition, Türkiye conducted sectorial risk assessments on, the Real Estate Agents (REAs) and Dealers in Precious Metals and Stones (DPMS) sectors identified as high risk according to Türkiye's NRA and MER to better fulfil the objective of conducting DNFBPs supervision on a risk-sensitive basis. Türkiye conducted as well, a "Legal person Risk Analysis" comprising of all legal person types (notaries, accountants, independent audit institutions, lawyers) in 2021 and prepared the supervision programmes accordingly. In addition, this analysis was updated in 2025.

Weighting and conclusion – Türkiye has addressed most of the deficiencies stated in the 2019 MER. There is still a remaining minor shortcoming as the fit & proper requirements do not extend to associates of criminals from being professionally accredited or holding (or being the beneficial owner

of) a significant or controlling interest in a DNFBP and a minor shortcoming on sanctions. Recommendation 28 is rated **largely compliant**.

Recommendation 29 – Financial Intelligence Units[89] (FIU)

In its 2019 MER, Türkiye was rated compliant with Recommendation 29.

Criterion 29.1 *Criterion rating*

MASAK is the Turkish FIU, organised within the administrative structure of the Ministry of Treasury and Finance and directly attached to the Minister. MASAK is an administrative style FIU and has the duty and power to collect data, receive suspicious transaction reports (STRs), analyse and evaluate them, to produce intelligence and to inform the relevant units of the intelligence produced and outcomes of the analyses, when necessary, in the scope of prevention of laundering proceeds of crime and financing of terrorism (PD 1, art. 231(1)(ç)).

Criterion 29.2

MASAK serves as the central agency for the receipt of STRs filed by obliged entities in the scope of prevention of laundering proceeds of crime and financing of terrorism (PD 1, art. 231(1)(ç)). The disclosures filed by reporting entities, include:

a) Suspicious transactions reports that obliged entities are required to report to MASAK (Law 5549, art.4(1)).
b) transactions, to which they are parties or intermediaries, exceeding the amount determined by the Ministry to MASAK (Law 5549, art.6).

Criterion 29.3

In relation to obtaining and accessing information, MASAK has:

a) the duty and the power to request all kinds of information and documents from (…) natural and legal persons, and unincorporated organisations" (Law no 5549 art. 7(1)). MASAK has the authority to request any information not only from obliged entities (reporting entities) but also from all natural and legal persons.
b) direct and indirect access to a wide range of financial, administrative and law enforcement information based on the access system given to MASAK to the data hold by public institutions and organisations (Law 5549, art. 9). Exceptions to this authority are public economic enterprises and the banks with public capital excluding the Central Bank of the Republic of Türkiye. Further, Law 5549 (art.16 (2)) indicates that the Customs Enforcement is obliged to report to MASAK suspicious cross-border currency declaration cases.

Criterion 29.4

In relation to analysis undertaken by the FIU:

a) MASAK conducts operational analysis. MASAK has the duty to analyse and evaluate STRs (PD 1, art.231(1)(ç)). Any reports and information received related to the prevention of laundering proceeds of crime and financing of terrorism should be evaluated by the MASAK expert staff (PD 1, art. 231 3 and 4). MASAK's analysis includes the use of statistical and analytical methods to obtain financial intelligence from the various data collected and other reports (ROE, art. 3(1)(b)). In

[89] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

addition, MASAK has the duty to examine the cases conveyed by Public Prosecutors and to fulfil the requests relating to the detection of the ML offence (PD 1, art. 231(1) (g, h)).

MASAK provides strategic analysis as it has the duty to research the subject matters of Law 5549 (PD1, art. 231 (1)c). MASAK carries out general analysis studies to determine general trends based on STRs and financial data for the purpose of preventing and detecting ML/TF offences. In addition, MASAK is mandated to produce financial intelligence by applying data analysis techniques on MASAK data warehouse and data obtained and accessed from various sources as well as to produce study reports on typologies, trends, patterns and profiles (MASAK Internal Circular dated 23 March 2017**).**

b) The instructions on how to report the findings of the analysis and which reports are to be written are contained in the MASAK Analysis Operations Directive. According to the aforementioned directive, main report types are identified as including but not limited with: Financial Analysis Report, Financial Detection Report, and Proceeds of Crime Report. (MASAK Analysis Operations Directive, art. 11).

Criterion 29.5

MASAK has the duty and the power "…to produce intelligence and to inform the relevant units of the intelligence produced and outcomes the analysis" (PD 1, art.231(1)(ç)) and "to convey cases to the competent Public Prosecutor's Office, where serious suspicion exists that a ML/TF offence has been committed" (PD 1, art.231(1)e). In addition, the public prosecutor may conduct any kind of exploration either directly or through the judicial law enforcement forces under his/her command in order to investigate (CPL, art.161). For this purpose, the prosecutor may demand all kinds of information from all public servants. This would include tasking MASAK with conducting financial intelligence analysis.

All information subject to dissemination are considered as official writings and measures that need to be taken and procedures to be followed to protect information have been determined by MASAK Internal Circular dated 23 October 2017.

Criterion 29.6

MASAK protects information in the following ways:

a) MASAK has policies and procedures in place to govern the security and confidentiality of information including the handling, storage, dissemination and protection of, and access to, information.
b) MASAK staff must obtain security clearances. In addition, employees of MASAK shall not disclose or make personal use of the information they access under penalty of law (Law No. 5549, art.22 (1 and 2)) and are obliged to sign a secrecy commitment declaration.
c) No person other that MASAK staff is allowed to enter MASAK premises.

Criterion 29.7

In relation to operational independence and autonomy:

a) MASAK is an administrative style FIU, organised within the administrative structure of the Ministry of Treasury and Finance and directly attached to the Minister. PD 1 provides a legal base for MASAK to carry out its functions free from any undue influence or interference. The authorities and powers are granted directly by the PD and Law No. 5549 and Law No. 6415. No body or institution therefore has the authority or position to interfere with MASAK's operations.
b) MASAK has a co-ordination role to exchange views and information for the prevention of the laundering of proceeds of crime (PD 1, art. 231(1)(a)). In addition, MASAK is authorised to exchange information and documents with its foreign counterparts and to sign Memorandum of

Understanding for those matters not included in the nature of an international agreement (PD 1, art. 231(1)L).

c) While MASAK resides within the Ministry of Treasury and Finance, MASAK has distinct core functions from the Ministry and has specific duties and powers (PD 1, art. 231(1)).

d) Article 231(1(n) of Presidential Decree No.1 grants MASAK the authority to request temporary assignment of personnel from other public institutions and organisations to MASAK, when their knowledge and expertise is necessary. In addition, MASAK is in a position to obtain and deploy the resources needed to carry out its functions.

Criterion 29.8

MASAK has been a member of the Egmont Group since 1998.

Weighting and conclusion – All criteria are met. **Recommendation 29 is rated compliant.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities[90]

In its 2019 MER, Türkiye was rated compliant with R.30.

Criterion 30.1

Public prosecutors are responsible for conducting criminal investigations, including ML, associate predicate offences and TF (CPL, art. 160-169) in Türkiye. Public prosecutors' offices (PPOs) operate in all 81 provinces independently. Each PPO is directed by a chief prosecutor who decides on the operational implementation of the national criminal policies designed by the MOJ. Since 2021 ML/TF investigations are carried out by specialised public prosecutors depending on the offence. Since 2023, Türkiye has established specialised ML bureaus in the PPOs located in the 15 metropolitan municipalities with the highest criminal indexes[91] where the allocation of higher ML specialised resources is needed. ML investigations are handled by regular public prosecutors -who are also trained in ML investigations- in the remaining 66 provinces. In addition, Türkiye has established one Counter Terrorism Bureau per province to investigate and prosecute all terrorism and TF-related cases. Each CT bureau includes at least one specialised TF prosecutor for the investigation phase and one for the trial phase. Public Prosecutors direct the investigation strategy and carry out their investigative duties with the operational support from LEAs, such as the Turkish National Police (TNP), General Command of Gendarmerie (GGC) , Customs Enforcement (CE) and the Coast Guard (CG) (CPL, art, 164 (1)).

LEAs have specialised proceeds of crime units to conduct ML/TF investigations, such as, the Türkiye National Police (TNP), Anti-Smuggling and Organised Crime Unit (KOM), Public Order, Counter Narcotics, Cyber Crimes and Migrant Smuggling Departments and the Turkish General Command of the Gendarmerie (GGC) KOM Unit. In 2022, the Ministry of Justice (MOJ) issued an internal circular disseminated to all governors of the 81 Türkiye cities, instructing LEAs under its competences (TNP, Gendarmerie and the Coast Guard Command) to prioritise ML/TF investigations (MOJ internal circular No. 2022/7). CE and CG does not have ML/TF special investigations units.

The TNP and GGC play a vital role in supporting prosecutors in terrorism and TF investigations, and in the prevention and disruption of these activities. The TNP General Directorate of Security is responsible for policing activities against all crimes in urban areas, while the GGC is the law enforcement unit operating in rural areas. Both institutions have special units dealing with TF. All TF units specialised in FETÖ-related

[90] Recommendation 30 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

[91] Ankara, Antalya, Adana, Bakırköy, Bursa, Diyarbakır, Gaziantep, Istanbul, Istanbul Anatolia, Izmir, Kayseri, Konya, Küçükçekmece, Mersin and Şanlıurfa.

cases, but TNP and GGC has a specialised sub-unit dealing with ISIL/AQ-related cases and another dealing with PKK/KCK-PYD/YPG cases given the differences in the nature of these actors and their financial management systems.

Criterion 30.2

In addition to the explained under c. 30.1, public prosecutors may conduct any kind of exploration with the support of LEAs including parallel financial investigations (CPL, art.160 & 161). For this purpose, the MOJ instructed LEAS to conduct parallel financial investigations in line with the identified national ML/TF risks, applying security measures and administrative sanctions for legal persons in case of ML/TF effectively, and ensuring specialization in the conduct of investigations (MOJ Circular 155/1). Consequently, TNP KOM and TEM send orders to all provincial units to conduct parallel financial investigations in TF/ML cases and to take the necessary measures to identify and seize the proceeds of crime using investigative techniques (TEM Order Letter and KOM Order Letter). Moreover, LEAs are responsible for investigating associate predicate offences in Türkiye under the public prosecutor command and are able to pursue parallel financial investigations related to ML regardless of where the offence occurred.

Furthermore, prior to seizure, MASAK, the Banking Regulation and Supervision Agency (BRSA), the Capital Markets Board (CMB), the Ministry of Treasury and Finance (MoTF), and/or the Public Oversight, Accounting and Auditing Standards Authority contribute to investigation or prosecution processes (CPL, art. 128).

Criterion 30.3

Türkiye has various designated competent authorities to expeditiously identify, trace and initiate freezing and seizing of criminal property and property of corresponding value.

Judicial authorities are empowered, either by a judge's order or, in urgent cases where delay would be prejudicial, by a prosecutor's order (CPL Art. 127(1)), to freeze and seize assets suspected to be criminal proceeds or intended for terrorist financing. Public prosecutors (CPL Art. 165) lead ML/TF investigations and instruct judicial police to conduct searches under Art. 119 where "delay would be prejudicial." They may order seizure of assets as evidence (CPL Art. 123) and pursue final confiscation under Art. 128–133.If there are cases that allow to assume that the person sought, or the evidence of the crime is located in the specified places, other people, belongings, homes, workplaces or other places belonging to them may also be searched. Items, found during the search are seized and their value is determined.

Assets which are deemed useful as a means of proof, or which constitute the subject of confiscation and proceeds of crime (including corresponding value) are to be frozen. If they are not surrendered voluntarily, they shall be seized (CPL, art.123). This seizure order is to be taken by the judge, however in cases where delay is prejudicial, the public prosecutor can take this measure.

In addition, MASAK identifies and traces proceeds of crimes and terrorist assets that may be subject to confiscation when performing its analysis, evaluation or examination on ML/TF upon (or without) the request from public prosecutors. MASAK may request for seizure of assets (Law No. 5549) in cases where there is strong suspicion that a money laundering offence is committed. The request for seizure is conveyed to relevant Public Prosecutor's Office (RoE, (art.11(1)). In ML/TF investigations, the Treasury and Finance Minister is authorised to suspend the transactions that are attempted to be conducted or currently going on within or through obliged parties for seven work days – extendable by a court order - or not to allow the performance of those transactions for the same period of time so that MASAK can verify the suspicion, analyse the transaction and convey the results of those analyses to competent authorities when necessary (Law No. 5549, art. 19/A)**.** MASAK is also responsible for conducting financial research regarding the decisions on freezing of assets in TF cases (Law No. 6415, art. 8 (1)) related to either domestic or international requests (Law No. 6415, art. 6 and 7).

Law No. 6415 (art. 3–7) establishes an inter-agency Assessment Commission within MASAK specifically to review TF freezing requests and instruct MASAK to implement them without delay.

Criterion 30.4

During the course of an investigation, public prosecutors can seize all identified assets where there are strong grounds for suspicion that they relate to proceeds of crime (CPL, art. 127 - 128). As indicated in Criterion 30.2, MASAK, BRSA, CMB, MoTF and Public Oversight, Accounting and Auditing Standards Authority are responsible for conducting financial analysis, evaluation and examination of predicate offences in the context of ML/FT. Additionally, the Tax Inspection Board (TIB), under the Tax Procedure Law No. 213, is empowered to investigate tax offences and refer any proceeds of financial crime to the public prosecutor.

Criterion 30.5

Türkiye has no specific anti-corruption enforcement authority. However, as mentioned in criterion 30.1, the authority of investigating all offences including corruption belongs to public prosecutors (CPL, art. 160-169).

Weighting and conclusion – All criteria are met. **Recommendation 30 is rated compliant.**

Recommendation 31 – Responsibilities of law enforcement and investigative authorities[92]

In the 2019 MER, Türkiye was rated largely compliant with R.31 because of minor deficiencies in the range of investigative techniques that competent authorities could use for ML and predicate offences.

Criterion 31.1

Competent authorities (public prosecutors) in charge of investigating all offences including ML, TF, and associated predicate offences (CPL, art. 160-169) have the powers to use compulsory measures, with the direct support or through other law enforcement authorities (Police, Gendarmerie, Customs Enforcement and Coast Guard) (CPL, art 161(2)), and MASAK (PD 1, art. 231(1)(g)) for:

a) the production of records held by FIs, DNFBPs and any natural or legal persons, as prosecutors may demand all kinds of information from all competent authorities and through them from all obliged entities (CPL, art. 161(1).
b) the search of persons and premises (CPL, art. 116-122), which includes the authority to search third party premises with the aim of apprehending a suspect or obtaining evidence.
c) taking witness and expert statements under oath (CPL, art. 43-61).
d) seizing and obtaining evidence (CPL, art. 123, 134; AML Law, art. 17). as prosecutors may demand all kinds of information from public servants and through them from obliged entities (CPL, art. 161(1).

Furthermore, MASAK may be tasked by the public prosecutor and is empowered to request information and documents from any public institution, organisation, natural or legal person, or unincorporated entity (Law No. 5549, art. 7).

[92] Recommendation 31 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

Criterion 31.2

Competent authorities conducting investigations can use a wide range of investigative techniques for the investigation of ML/TF and associated predicate offences (though controlled delivery limited to certain offences), including:

a) undercover operations for ML/TF investigations (AML Law, art. 17 (3)) (TF Law No. 6415 (c). Undercover operations can also be applied to other associated predicate offences, such as manufacturing and trading of narcotics or stimulants, organise crime, armed organisations or supplying weapons to these organisations and crimes related to the protection of cultural and natural substances.

b) intercepting communications, wiretapping and recording of communications (CPL, art. 135) and monitoring with technical devises (CPL, art. 140) for specific crimes including ML (CPL, art. 135 (8)) and TF (TF Law, art. 8 (b)) and associate predicate offences (CPL, art. 135 (8) 1-16).

c) accessing computer systems, its stored contents and archives, and for copying, analysing and transcription into written form of computer records (CPL, art. 134).

d) controlled delivery limited to drug trafficking, smuggling, ML and TF cases (Law No. 4208, art. 2, 10, 11 and 13; AML Law, art. 17(3); TF Law, art. 4(8)(ç)) for the purpose of identifying the perpetrators, finding out and collecting all kind of evidence and confiscating the smuggled or suspected to be smuggled goods and funds.

Criterion 31.3

Türkiye ensures that competent authorities (prosecutors, LEAs, MASAK) have timely access to a wide range of information, particularly to support the identification and tracing of criminal property and property of corresponding value.

Türkiye has mechanisms in place to:

(a) identify whether natural or legal persons hold or controls accounts. The CPL entitles public prosecutors to conduct any kind of inquiry directly or through judicial law enforcement officers and request any kind of information from all public officials. To ensure data confidentiality is respected in the acquisition of information, the authority of public prosecutor covers the identification of accounts held or controlled by real or legal persons and procedural actions in investigation stage should be conducted in secrecy (with due care for information (CPL, art. 157(1))).

(b) Public prosecutors have the authority to request and obtain any information from public and private institutions who hold asset records without prior notification to the owner. When operations need to be conducted outside the judicial environment, a Public Prosecutor may also request other Public Prosecutors to carry out relevant operations (CPL, art. 161). Public Prosecutors will request this information through judicial law enforcement authorities (Police, Gendarmerie, Customs administration and Coast Guard).

MASAK and other competent authorities also play a significant role in identifying, tracing, and evaluating property subject to confiscation ad they have authority to request all kinds of information and documents from public institutions and organisations, natural and legal persons, and unincorporated organisations directly (without requiring an order from public prosecutor or judge) during its analysis, evaluation or examination phase (CPL, art. 164 and 165). MASAK (and examiners either from MASAK or other competent authorities assigned to the effect) is also obliged not to induce disclosure as the Law prohibits the disclosure of secrets acquired while exercising duties, about the persons, transactions and account statements, businesses, enterprises, wealth and professions of the individuals and others related to them. This confidentiality requirement also supports the ability to identify and trace assets without prior notification to the owner (Law No. 5549, art. 22(1)).

Criterion 31.4

Competent authorities (public prosecutors) in charge of conducting investigations of ML/TF and associated predicate offences can request any information from public entities in the context of an investigation (CPL, art. 161 (1)), including from MASAK, Türkiye's FIU. Moreover, MASAK is obliged to examine the cases conveyed by Public Prosecutors and to fulfil their requests relating to the detection of money laundering offences (PD No.1, art. 231(1)(h))

In addition, MASAK carries out analysis, evaluation or examination on ML/TF upon the request from public prosecutor and on its own initiative as indicated in Criteria 30.2**. These activities form an integral part of the public prosecutor's investigation.** In the course of this work, MASAK and examiners have the duty and the power to request all kinds of information and documents from natural and legal persons, and unincorporated organisations (PD 1, art. 231(1)(j)). MASAK has the authority to request any information not only from obliged entities (reporting entities) but also directly from all other natural and legal persons.

> *Weighting and conclusion –* Türkiye has the legal framework, powers and mechanisms in place for a wide range of investigative techniques and information that competent authorities can use for ML, TF and some (but not all) associated predicate offenses. **Recommendation 31 is rated largely compliant**

Recommendation 32 – Cash Couriers[93]

In its 2019 MER, Türkiye was rated largely compliant with R.32.

Criterion 32.1

Türkiye has implemented a hybrid system; a disclosure and a declaration system for the physical cross-border transportation of Turkish currency, foreign currency or instruments[94]. Passengers shall declare Turkish currency and foreign currency and instruments for the purpose of exchange control as described in c.32.2. In addition, passengers making a physical cross-border transportation of Turkish currency, foreign currency or instruments shall disclose them fully and accurately upon the request of Customs Enforcement Türkiye have measures in place to deal with the cross-border transportation of Turkish currency, foreign currency or instruments through mail and cargo.

Criterion 32.2

Turkish currency and the BNIs enabling payments in Turkish currency exceeding TRY 185 000 (approx. EUR 5 070), foreign exchange exceeding EUR 10 000 and its equivalent must be declared for outgoing cross border transportation to the Customs Enforcement by Cash Declaration Form. (Circular, 2024/01 2.1). This provision intends to protect the value of the Turkish Currency. This provision is applicable to that "carried by passengers physically, in their baggage or vehicles". Incoming cross border transfers of Turkish currency, foreign currency or instruments related to export payments, profit obtained from transit trade, foreign capital and cash obtained from other origins, should be declared to the Customs Enforcement. Cash transfers to Türkiye relating to personal capital and liabilities such as gifts, donations, dowry and other transfers detailed within Decree No.32 on the protection of the value of Turkish Currency and the Decree

[93] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

[94] Turkish currency instruments and foreign currency defined in Decree 32, art.2, covers Turkish money and all kind of instruments and means enabling payments in Turkish currency such as commercial and ordinary bills, letters of credit, credit cards, traveller cheques, remittances and letters in addition to foreign currency banknotes.

on Regulation and Supervision of Foreign Trade of Rough Diamond must be transferred to the country only through the banking system.

Criterion 32.3

Travelers making a physical cross-border transportation of Turkish currency, foreign currency or instruments ensuring payment by them, shall disclose them fully and accurately upon the request of Customs Enforcement (Law 5549, art.16(1)). In order to enhance awareness and ensure deterrence during the entry into or exit from the country, the Customs Enforcement may require passengers to disclose amount and provide explanations concerning the source of the cash they are carrying. The passengers to be subject to such controls shall be selected based on risk analysis which may consider information received from relevant institutions or based on the assessment of authorized personnel (Cash Controls Circular No 2024/01 art 4(3)).

Criterion 32.4

Upon discovery of a false or misleading disclosure or failure to disclose, passengers are required to give information about identity, profession or occupation, address of residence, destination address and telephone number, the values with passengers concerning their type, quantity, amount, source, purpose of use and to whom they belong, detailed list of values held by the passenger determined by customs officer (ROM, art.42 and Cash Controls Circular, art. 2.3.). In addition, in the event that the Customs Enforcement requests an explanation from the passenger entering or leaving the country, if no explanation is made or if it is determined that a false or misleading explanation is made, the Customs Enforcement shall impose an administrative fine of 10% of the undisclosed amount in accordance with Article 16 of the Law No. 5549 on the Prevention of Laundering Proceeds of Crime; all cash accompanying the passenger shall be taken under custody and a copy of the Cash Disclosure Record regarding the transaction shall be sent to MASAK and relevant competent authorities. (Cash Controls Circular No 2024/01, art. 3.3., AML Law art. 16(2)).

Criterion 32.5

Persons who make a false disclosure are subject to an administrative fine equal to one tenth of the difference between the value carried along and the value disclosed (ROM art.43(2)) This amount appears to be small. In addition, values carried along by travellers may be sequestered by the Customs Enforcement. The case is conveyed to MASAK as suspicious. MASAK carries out analysis and evaluation work for the case. In addition, if custom officials consider the case to be criminal, they will convey the case to the Public Prosecutor immediately. Where a seizure was made without a warrant of a judge, the seizure shall be submitted to the judge who has jurisdiction for continued authorisation within 24 hours. Criminal sanctions can be applied including confiscation of the values and imprisonment. Penalties overall could be considered proportionate and dissuasive only when the case is dealt in the scope of other laws.

Criterion 32.6

Information obtained through the declaration and disclosure systems is shared with MASAK (Law 5549, art.16 and ROM art. 43(1)). In addition, MASAK signed a protocol with the Ministry of Trade that ensures MASAK receives information on cross border movements of cash amounts electronically.

Criterion 32.7

Border protection, customs regulation and migration policies are managed primarily by the Ministry of Trade and Ministry of Interior. Nationwide co-ordination mechanisms are in place to share intelligence in relation to cash couriers with other LEAs. Bulk transfer of cash is managed through the Central Bank and there is a single window exchange mechanism enabling exchange of information between the central bank and LEAs in this regard.

Criterion 32.8

Customs can restrain currency or BNI when there is suspicion of any offence based on the general provision in CPL, art. 123 where "materials likely to be useful as means of proof or values of property which are subject to confiscation of goods, or confiscation of gains shall be secured". In addition, where there is "strong" suspicion that ML/TF offences are committed, the asset values may be seized (Law 5549, art.17). In addition, Public Prosecutor may also make seizure decision in urgent cases. The seizure applied without the judicial decision is submitted for the approval of the judge on duty within twenty-four hours at the latest.

In cases no explanations are made, or false or misleading explanation is made in the scope of declaration or disclosure, all values carried by the travellers are stopped and sequestered by the Customs Enforcement. MASAK is notified of cases which are deemed to be suspicious. (Law 5548, art.16(2) – RoM, art. 43).

Criterion 32.9

The Turkish declaration and disclosure systems allows for international co-operation and assistance. Customs has MoUs with partners overseas enabling the sharing of information. Declarations and disclosures are filed on central system and retained by MASAK, which is authorised to exchange information including cash declarations and disclosures to international partners. Information is shared by the Directorate General of Customs Enforcement, Ministry of Trade through its Mutual Administrative Assistance Agreements signed with over 70 countries and assistance may be sought/provided through the MLA route.

Criterion 32.10

The use of data and information collected through disclosure and declaration systems is safeguarded by various principles; Protection of personal data, protection of information by Customs Enforcement and other laws.

Criterion 32.11

Persons transporting funds or BNIs in relation to ML/TF or predicate offences may be subject to sanction for these offences. MASAK is required to open a file where a referral is made and currency or BNIs may be subject to seizure only where 'strong suspicion' exists (For more details see criterion 32.5). Where a criminal investigation is started measures under Rec 4 are engaged and enable the confiscation of currency or BNIs.

> ***Weighting and conclusion –*** Türkiye has some minor deficiencies as regards to sanctions for false declaration/disclosure in addition to some shortcoming to sanctions to persons carrying out cross border transportations of currency or BNI related to ML/TF offences or predicate offences. Recommendation 32 is rated **largely compliant**.

Recommendation 33 – Statistics[95]

In its 2019 MER, Türkiye was rated largely compliant with R.33 and has continued to develop statistics.

Criterion 33.1

a) Türkiye maintains comprehensive statistics regarding STRs received and disseminated including breakdown according to sectors.
b) Türkiye does not maintain comprehensive statistics on ML/TF investigation. While statistics on ML and TF prosecution and convictions were provided, Türkiye was unable to provide full detail of

[95] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

Terrorism cases where TF has been an aspect of the prosecution or conviction without a manual review.

c) Statistics for property frozen, seized and confiscated is held across a number of LEAs, MASAK and Courts with different systems in place each providing statistics for a single strand. In accordance with the fourth strategic objective of AML/CFT Strategy Document, all competent authorities in Türkiye closely monitor the effectiveness on seizure and confiscation practices. Thanks to the UYAP database, after Türkiye's 2019 MER, many statistics are produced and justice policies are determined using the statistics produced. Recent improvements to UYAP (The National Judiciary Informatics System) in line with strategic objective 4 of the Strategy Document allow for the tracking of certain seizure and confiscation statistics. Work has been carried out on the relevant UYAP fields to record the value of the properties and assets which have been seized or confiscated during investigations and prosecutions.

a) Türkiye maintain statistics on MLA requests for co-operation made and received.

Weighting and conclusion – The setting up of the UYAP system improved the collection, centralisation and upkeep of statistics since Türkiye's 2019 MER. **Recommendation 33 is rated largely compliant.**

Recommendation 34 – Guidance and Feedback [96]

In its 2019 MER, Türkiye was rated largely compliant with R.34 especially because guidance did not cover the full range of competent authorities, supervisors and SRBs but Türkiye has expanded the coverage of guidelines since its 2019 MER to for example, cover lawyers.

Criterion 34.1

Guidance

MASAK is the main authority tasked with providing AML/CFT guidance to obliged entities. MASAK carries out its duty by publishing guidance and leaflets, and providing feedback through formal writings, workshops and its website. Between 2013-2023, MASAK circulated 12 General Communiqués [97] related to AML/CFT, published 12 booklets on the Turkish AML/CFT framework and liabilities of obliged entities as well as guidelines on STR submissions for banks and the Postal and Telegraph Corporation (PTT), capital market intermediary institutions, insurance and pension companies, factoring, financing and financial leasing companies, exchange offices, payment service providers, electronic money institutions, VASPs and other obliged entities. A general FAQ related specifically to AML/CFT responsibilities of obliged entities is also available on MASAK's public website.

MASAK has also prepared brochures for savings finance companies, VASPs, lawyers, notaries, those engaged in the purchase and sale of real estate for commercial purposes and those intermediating these transactions (real estate agents), those engaged in the purchase and sale of all types of sea, air and land transportation vehicles, including construction machinery, buyers and sellers of precious metals, stones or jewellery and authorised institutions specified in foreign exchange legislation (foreign exchange offices).

In order to improve the framework on financial analysis and investigation, in 2022 LEAs issued financial investigation guidelines. MASAK also prepared a Financial Analysis Guideline. MASAK and other relevant competent authorities have given weight on guidance activities to increase awareness of obliged parties,

[96] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

[97] This includes 'core' communiqués such as Communiqués 5, 12, 13, 19, 20 and 21, as well as 'lesser' communiqués that amend or make other minor changes to previously released communiqués.

citizens and examiners. For example, based on the results of 2023 NRA which was prepared in line with the Strategic Objective II of AML/CFT Strategy Document, Typology Reports (for official use) were prepared and disseminated to competent authorities in 2023, in order to further comply with the FATF standards (e.g. action 1.5 of the NRA Action Plan).

Aside from the restricted ones, most of the guidelines can be accessed from the official website via the link https://masak.hmb.gov.tr/rehberler.

Feedback

MASAK provides feedback on STRs and publishes STR statistics, methods, trends and case studies through annual activity reports, guidelines and periodicals for the purpose of training (RoM, art. 30). Within this framework, obliged entities reporting suspicious transaction are informed by MASAK when the report is recorded. MASAK also provides feedback in face-to-face interactions with obliged entities, including via annual workshops and other trainings.

Workshops are used to inform compliance officers about AML/CFT developments and trends and to provide general feedback about STRs in terms of quality, quantity and other trends. Trainings cover a range of AML/CFT topics, including typologies and STR trends. Between 2020 and 2024, trainings were organised for all FIs including the PTT and other DNFBPs, such as notaries, accountants and dealers in precious metals and stones. Separately, MASAK also organises various seminars and conferences to provide further information, including case studies. Periodic emails to obliged entities on the results of STR analysis are circulated; annual activity reports are available on the MASAK website; and sanitised case studies are also published.

This does not cover the full range of competent authorities, supervisors and SRBs but has expanded since 2019.

> *Weighting and conclusion –* Full range of competent authorities and SRBs were not involved in the establishment of guidance but guidance has expanded since 2019 to for example cover lawyers. **Recommendation 34 is rated largely compliant.**

Recommendation 35 – Sanctions[98]

Türkiye was rated partially compliant with R.35 in its 2019 MER and re-rated largely compliant in its 2021 FUR.

Criterion 35.1

Türkiye has a range of proportionate and dissuasive sanctions whether criminal, civil or administrative, available to deal with natural or legal persons that fail to comply with the AML/CFT requirements of Recommendations 6 and 8 to 23. Core sanctions applicable to natural or legal persons that fail to comply with AML/CFT requirements in Türkiye are found in AML Law, arts. 13, 14 and TF Law art. 15 and their amount is updated on a yearly basis. On Targeted Financial Sanctions (R6): Maximum administrative penalty is TRY 15 111 620 [EUR 414 243], Additionally, according to the same article, the fines imposed cannot be less than the amount of the transaction. For example, if a legal person is found to have conducted a transaction of EUR 2 million infringing TFS, it will be fined EUR 2 million. Therefore, in practice,

[98] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019 and 2021 FUR, with minor non-substantive edits included from Türkiye.

administrative fines in TFS cases have no upper limit. Non-Profit Organisations (R8): Penalty for collecting aid without authorisation ranges from TRY 37 770 to 755 574 [from EUR 1 035 to EUR 20 712].

A statute of limitations restricts the ability to levy administrative fines to within eight years from the date of violation of the obligation: art. 13.6, AML Law.

Administrative fine for legal persons who fail to comply with CDD, and periodic reporting obligations are TRY 226 671 (EUR 6 213), for fail to STR filling is TRY 377 783 (EUR 10 355). This fine is doubled for any FI in breach of its AML/CFT obligations.

Obliged entities that fail to comply with "training, internal control, control and risk management systems" obligations are given, at least, 30 days in order to remove deficiencies and take necessary measures. After this grace period, failing the removal of cited deficiencies, an administrative fine of TRY 3 777 658 (EUR 103 554) is levied. For financial institutions, this fine is applied twofold.

Individuals, institutions and organisations that fail to comply with the obligations of electronic notification specified in art. 9/A of this Law are sanctioned with an administrative fine of TRY 302 229 (EUR 8 284) for each failure to comply. The total amount of administrative fine applied in one year cannot exceed TRY 7 555 808 (EUR 207 121).

In regard to "tipping off," record keeping and providing information when requested, sanctions available include imprisonment from 1 to 3 years and a judicial fine up to 5 000 days (TRY 2 500 000 or EUR 68 530) for natural persons. Legal institutions that fail to provide information and documents upon request face the cancellation of their license to operate and confiscation of assets and gains: TCL, arts. 54, 55, 60.1 and 60.2.

Individuals who do not obey or who neglect or delay to implement asset freezing measures taken in pursuance to applicable TFS are punished by an imprisonment for a term of six months to two years or a judicial fine of TRY 18 000 (EUR 493) to TRY 365 000 (EUR 10 005), unless such act constitutes a serious offence requiring a heavier penalty[99]. In the case where the entity is a legal entity or a representative of a legal person; or a person, who is not the entity or representative, but undertakes a duty within the scope of that legal person's operational framework, this legal person is punished by an administrative fine between TRY 75 553 (EUR 2 071) and TRY 15 111 620 (EUR 41 436). See analysis for NPOs under c.8.4(b).

Criterion 35.2

Individuals that have responsibility for AML/CFT obligations within legal entities, including directors and senior managers, may be held in full or in part personally liable for the administrative fine imposed on the obliged entity: Law No. 6098, art. 400. Furthermore, directors and senior management who do not conform to, or who neglect or delay to obey, asset freezing decisions taken in pursuance to UNSCR 1267/1989, 1988 and 1373 are punished by imprisonment for a term of six months to two years or a judicial fine (TRY 18 000 to TRY 365 000 - approx. EUR 493 to 10 005) unless such act constitutes a serious offence requiring a heavier penalty: TF Law, art.15 and TCL, art.52.

> ***Weighting and conclusion –*** Türkiye has a range of proportionate and dissuasive sanctions whether criminal, civil or administrative, available to deal with natural or legal persons that fail to comply with the AML/CFT requirements of Recommendations 6 and 8 to 23. There is also an eight-year time limitation concerning the right for supervisors to impose administrative fines. **Recommendation 35 is rated largely compliant**.

[99] "*Conceptual aggregation*" is a general principle in the Turkish Criminal System. If a natural or legal person commits two distinct offences at the same time as a single act, the individual is punished according to the offence requiring a heavier penalty. For example, an individual that delays the implementation of asset freezing measures taken in pursuance to applicable targeted financial sanctions may also be considered as reaching the threshold for financing, aiding or abetting terrorism. Accordingly, the individual would be liable to sentencing under the heaviest sanction available.

Recommendation 36 – International instruments[100] [101]

In its 2019 MER, Türkiye was rated largely compliant with R.36 because of some technical shortcomings related to R.3, R.5, R.28 and R.31. Minor shortcomings remain related to R. 3 and R.5.

Criterion 36.1

Türkiye has signed and ratified the Vienna Convention, the Palermo Convention[102], the TF Convention and the Merida Convention.

Criterion 36.2

Türkiye has implemented the vast majority of the relevant provisions of the Palermo Convention, Vienna Convention, Merida Convention and the TF Convention. However, there are a number of technical gaps with the relevant elements of the conventions (see R.3 and R.5).

> *Weighting and conclusion –* Minor technical gaps with the relevant elements of the conventions prevent full compliance with R.36. **Recommendation 36 is rated largely compliant**.

Recommendation 37 – Mutual legal assistance[103]

In its 2019 MER, Türkiye was rated compliant with R.37.

Criterion 37.1

In addition to the bilateral and multilateral agreements on mutual legal assistance to which Türkiye is party, Türkiye has a legal basis in the International Judicial Co-operation in Criminal Matters Law (IJCL). While executing the request for judicial co-operation, the provisions of the Turkish Criminal Procedure Law (TCPL) shall apply if there are no relevant provisions within the IJCL or other laws (IJCL, art. 5).

Criterion 37.2

The IJCL identifies the Ministry of Justice (MoJ) as the central authority. The Directorate General for Foreign Relations and European Union within the MoJ is responsible for MLA. The MoJ uses a National Judiciary Informatics System (UYAP) to track and execute its work. The system is capable of filtering various files based on a coding system, which would allow for the prioritisation of case files. In addition, this system helps in communicating the requests to the judicial authorities in different locations in Türkiye. It also helps to prioritise the requests so that urgent cases are notified through UYAP system.

[100] The UNCAC Implementation Review Mechanism (IRM), for which the UNODC serves as secretariat, is responsible for assessing the implementation of the UNCAC. The FATF assesses compliance with FATF Recommendation 36 which, in relation to the UNCAC, has a narrower scope and focus. In some cases, the findings may differ due to differences in the FATF and the IRM's respective methodologies, objectives and scope of the standards.

[101] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019, with minor non-substantive edits included from Türkiye.

[102] The following components of the Palermo Convention were adopted by Türkiye by laws No. 4800, 4803 and 4804 on 2003-02-04 and ratified by the Decree of the Council of Ministers No. 2003/5329 on 2003-03-18: (i) Protocol against the Smuggling of Migrants by Land, Air & Sea and (ii) Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children. The component of the Palermo Convention - Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition – was adopted by Türkiye by law No. 5095 on 2004-02-17 and ratified by the Decree of the Council of Ministers No. 2004/7097 on 2004-04-26.

[103] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019.

Criterion 37.3

Türkiye does not subject MLA requests to unreasonable or unduly restrictive conditions. The reasons for denying a request are as follows (IJCL, art. 4):

The sovereign rights, national security, public order or other fundamental interests of Türkiye are violated.

The offence subject to the request is solely a military offence, thought crime, political offence or an offence connected with a political offence.

There are convincing grounds that the person subject to the request would be exposed to an investigation or prosecution or be punished or be exposed to torture or ill-treatment because of his/her race, ethnic origin, religion, nationality, connection to a certain social group or political opinions.

Fundamental guarantees in relation to the right to defence are not granted in the requesting State.

Criterion 37.4

Türkiye does not refuse MLA requests solely on the basis that the offence involves fiscal matters (IJCL, art. 4). Secrecy or confidentiality does not constitute a ground for denying a request.

Criterion 37.5

Türkiye maintains the confidentiality of MLA requests, as the IJCL indicates that while executing the request for judicial co-operation, the provisions of the TCPL shall be applied, if there are no relevant provisions within the IJCL, and the TCPL addresses the secrecy (duty of care, protection of information) of investigation (art. 157).

Criterion 37.6

Article 4 of the IJCL outlines the grounds for possible rejection and lack of dual criminality is not such a ground unless it involves coercive action such as search and seizure (IJCL. art.8(1)(ç)).

Criterion 37.7

Where dual criminality is required for MLA, the broadest possible interpretation is used, and it is sufficient that both countries criminalise the conduct underlying the offence.

Criterion 37.8

While executing the request for judicial co-operation, the provisions of the TCPL shall be applied if there are no relevant provisions within the IJCL or other laws (see R.31) (IJCL, art. 5).

Weighting and conclusion – All criteria are met. **Recommendation 37 is rated compliant.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation[104]

In its 2019 MER, Türkiye was rated compliant with R.38. Türkiye is being assessed following changes to R. 38 which now require countries to: provide co-operation on identifying, tracing, evaluating, investigating, freezing, seizing and confiscating criminal property and property of corresponding value; recognise and enforce foreign confiscation and freezing orders without requiring a domestic investigation; have mechanisms to manage, preserve and dispose of assets at all stages of cross-border asset recovery; enable informal communication in asset recovery cases; and have the ability to share confiscated assets with other countries, particularly where co-ordination led to the confiscation.

[104] Recommendation 38 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

Criterion 38.1

Türkiye has measures, including legislative measures, to take action in response to requests for co-operation by foreign countries seeking assistance to identify, trace, evaluate, investigate, freeze, seize and confiscate criminal property and property of corresponding value. Key legal instruments include the Criminal Procedure Code (art. 116-134) on search and seizure, the Turkish Penal Code, (art. 54 and 55) on confiscation of property and gains, and art. 54 (2) and 55(2) which allow for confiscation of property of corresponding value. Additionally, under the AML Law (art. 19 (A)), the Minister of Treasury and Finance may suspend transactions for seven working days upon request from a foreign authority. Provisions also allow Turkish authorities to provisionally seize assets in urgent cases—even before an MLA request is formally received—if there is a risk that the evidence may be lost or destroyed IJCL art. 8(2)).

Assistance is also provided by Türkiye on the basis of various multilateral conventions and bilateral treaties, all of which are directly applicable under the Constitution, art. 90. In this regard, Türkiye participates in regional and global co-operation networks including the Southeast European Law Enforcement Centre (SELEC), the Southeast European Prosecutors Advisory Group (SEEPAG), the Camden Asset Recovery Iner-Agency Network (CARIN) Asset Recovery Inter-Agency Network (ARIN), INTERPOL, European Union Agency for Criminal Justice (Eurojust) and the European Judicial Network (EJN). Workgroups and liaison points have been established to facilitate prompt responses to foreign co-operation requests. Justice counsellors posted abroad engage directly with counterpart authorities to enable rapid and informal assistance, while seven "Offices for International Judicial Co-operation in Criminal Matters" have been established in high-volume courthouses to enhance domestic co-ordination. Where no treaty exists, Türkiye can execute requests on the basis of reciprocity (Circular No. 69/2). The Assessment Team also recognised other informal mechanisms (electronic mail) used by Türkiye to assist and seek assistance from countries. Within the international co-operation framework, there is however no legislative obligation to expeditiously respond to requests except as it relates to the Egmont Group, the Charter of which mandates that members (FIUs) should, in the first instance, reply to requests within 30 days. The minor shortcomings in c.3.1 and 3.7 may also slightly limit the range of assistance that can be provided.

Criterion 38.2

Türkiye's legal and institutional framework enables the recognition and enforcement of non-conviction based foreign confiscation and provisional measures in line with R.4 and Law No. 6706 which regulates international co-operation procedures (c.4.9 and c. 38.1 refer) through, among others, continuation of proceedings. Under Turkish law, a fundamental principle of the domestic legal framework is that a confiscation decision can only be rendered following the commission of an intentional offence, as set out in the Turkish Criminal Law (TCL, art. 54).

The law also provides for the continuation of proceedings and the confiscation of assets, including material gains and other property subject to confiscation, in cases where the suspect is deceased (TCL, art. 64). In addition, these measures are also executed under the Council of Europe Conventions, such as the European Convention on the International Validity of Criminal Judgments (CETS 70), the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime and on the Financing of Terrorism (CETS 198), the Criminal Law Convention on Corruption, as well as under bilateral agreements, including those concluded between Türkiye and Brazil, the United States and Romania.

Also, even when a bilateral or multilateral international agreement is not available, judicial co-operation requests of foreign states, subject to the principle of reciprocity, may be accepted.

Where a request is received, recognition is given to the order, without having to secure a national confiscation order, however there is a requirement to first verify the order for its compliance with international treaties and then have the central authority conduct a review in a formal or structured manner.

Further, the execution of a request for judicial co-operation from a foreign State may be subjected to a condition or guarantee by the central authority (IJCL art. 3).

Criterion 38.3

Türkiye is not required to initiate a domestic investigation to enforce foreign confiscation orders. The central authority evaluates, decides on and determines the type of the judicial co-operation and method to be followed IJCL art. 3 (1) (a)(b). This enables reliance on the findings of fact in foreign orders and such approach has been followed in at least one request.

Criterion 38.4

Where the requested country requires a court order to provide assistance due to fundamental principles of domestic law or other considerations, Türkiye would be able to issue such an order as Turkish judicial authorities may request assistance in matters needed at any stage of the investigation IJCL art. 7 and 8). In relation to assets and values in foreign countries, seizure and confiscation decisions of Turkish judicial authorities are subject to legal review under Turkish law, irrespective of the fact that the property or the value is abroad. As it would be a Turkish judicial authority that rules on the seizure or confiscation decision, there is no obstacle to seeking a legal remedy on the merits.

Criterion 38.5

Türkiye has a legal framework that facilitates the application of domestic mechanisms for managing, preserving and disposing of assets (c. 4.11 refers). These mechanisms can be extended to cross-border co-operation as requests are treated in accordance with Turkish Law, including provisions to preserve assets, and the Criminal Procedure Code applies for any cases not explicitly provided in the IJCL art. 5 and 8 and Criminal Procedure Code, art. 132). The provisions of the Regulation on Property of Crime would also apply.

Criterion 38.6

a) Türkiye has measures to enable informal communication in asset recovery cases. Competent authorities actively participate in regional and international co-operation mechanisms such as the SELEC, SEEPAG, CARIN, ARIN, INTERPOL, Eurojust and the EJN. Türkiye has appointed designated contact points for Eurojust and EJN and uses the INTERPOL I-24/7 system for secure and rapid information exchange. Additionally, Türkiye is engaged in co-operation through the Consultative Council of European Judges (CCJE), the Consultative Council of European Prosecutors (CCPE) and the International Association of Prosecutors (IAP). These networks include working groups and liaison points that support rapid responses to foreign co-operation requests. Justice counsellors and liaison officers based in overseas missions play a key role in maintaining real-time, verbal and informal communication with foreign counterparts. Within the scope of international judicial co-operation procedures, Turkish judicial authorities are required to request annual confirmation from the requesting state on whether asset freezing or seizure measures should remain in place IJCL art. 8). To complement this mandate, Türkiye's UYAP systems provides a coding mechanism and there is a clerk who is designated to follow-up on requests pertaining to assets.

b) Türkiye has the authority for competent authorities to provide further related assistance without requiring a supplemental request. Turkish judicial authorities are required to transmit relevant information to foreign states when it may be useful for initiating an investigation, even in the absence of a request IJCL art. 7 (2).)

Criterion 38.7

a) Türkiye has treaty-based mechanisms which facilitate the sharing of confiscated assets with other countries. Türkiye has entered into bilateral agreements with a number of countries—including the United States, China, Russia, Kazakhstan and several others—which expressly allow for the sharing

of confiscated proceeds resulting from judicial co-operation. In the absence of a treaty, Türkiye may still accept and act on co-operation requests based on reciprocity (LIJCCM, art. 3).

b) Türkiye has measures in place to allow for the deduction or sharing of substantial or extraordinary costs associated with executing freezing, seizure or confiscation orders. Legislation provides that unless otherwise agreed by the parties, costs incurred in executing a request for judicial co-operation are to be borne by the executing state (IJCCM, art. 34 (1)). The IJCCM (art. 34 (2) and bilateral agreements mentioned under sub-criterion (a) contain specific provisions addressing the allocation or reimbursement of extraordinary costs.

Criterion 38.8

Türkiye has in place a broad network of multilateral and bilateral instruments to enhance co-operation in asset recovery. It is a party to all key multilateral conventions relevant to asset recovery, including the United Nations Convention against Corruption, the UN Convention against Transnational Organized Crime, the UN Convention against Illicit Traffic in Narcotic Drugs and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime and on the Financing of Terrorism (CETS 198). Türkiye has also ratified other European legal instruments such as the European Convention on Mutual Assistance in Criminal Matters (CETS 30), its Second Additional Protocol (CETS 182), the European Convention on the Transfer of Proceedings in Criminal Matters (ETS No. 073) and the European Convention on the International Validity of Criminal Judgments (CETS 70). In addition to its multilateral commitments, Türkiye has concluded bilateral MLA treaties that include provisions for the detection, freezing, seizure, and confiscation of assets with at least 13 countries, including the United States, China, Morocco, Iraq and Romania. These agreements support Türkiye's capacity to respond to and request co-operation in asset recovery cases, even with jurisdictions outside of regional multilateral frameworks.

Türkiye's co-operation is further supported by active participation in a wide range of operational and expert-based networks, including CARIN and ARINs. Justice counsellors and designated bilateral contact points help facilitate fast and informal communication without the need for formal correspondence.

> *Weighting and conclusion –* Türkiye has a strong framework including legislation and active participation in different mechanisms for asset freezing, seizing and confiscation. Minor shortcomings remain as, except for the FIU, there is no explicit obligation in law to expeditiously respond to requests, and deficiencies under c. 3.1 and c. 3.7 cascade. **Recommendation 38 is rated largely compliant.**

Recommendation 39 – Extradition[105]

In its 2019 MER, Türkiye was rated compliant with R.39.

Criterion 39.1

Türkiye can execute extradition requests in relation to ML/TF without undue delay:

a) ML and TF are extraditable offences under Turkish law, provided the upper limit of the sentence of imprisonment is at least one year according to both the law of the requesting State and Turkish law. ML and TF offences carry such a sentence in Türkiye.

b) MoJ is the Central Authority in extradition procedures. The MoJ uses a National Judiciary Informatics System (UYAP) to track and execute its work. The system is capable of filtering various files based on a coding system, which would allow for the prioritisation of files. There is also the Circular dated 16 November 2011 and numbered 69/4, which is the guide for the practitioners on

[105] This Recommendation was not under review. Therefore, the text for the Recommendation is copied from MER 2019 with minor editorial enhancements.

extradition. Türkiye does not place unreasonable or unduly restrictive conditions on the execution of requests, with conditions under which extradition can be denied being clearly defined (IJCL, art. 11).

Criterion 39.2

Turkish nationals are not eligible for extradition, except for the obligations related to being a party to the International Criminal Court (IJCL, art.11). If the extradition request is refused on the ground of nationality, the relevant judicial authority (Public Prosecution Office) is notified for initiation of an investigation against the person sought to be extradited. In addition, in line with art. 6 of the European Convention on Extradition and upon request of the country, cases are conveyed to Turkish judicial authorities without undue delay for initiation of a judicial investigation in the case where the extradition request is rejected on the ground of nationality.

Criterion 39.3

In Türkiye, the extradition request may be accepted for offences which require the upper limit of the sentence of imprisonment to be at least one year according to both the law of the requesting State and Turkish law, during the investigation or prosecution phase. If already convicted, the extradition request may be accepted if the imposed sentence is an imprisonment for at least four months (IJCL, art.10). Although dual criminality is required in some cases, Türkiye takes a conduct-based approach to dual criminality. The jurisdiction indicates that this principle is practised in a flexible manner and it is rarely used as a ground for refusal. There is no requirement for the category of the offence to be identical in both countries and authorities can use the description of criminal conduct in domestic law, which most resembles the crime being presented.

Criterion 39.4

The extradition process is simplified when the person, subject to the extradition request, consents (IJCL, art. 17).

Weighting and conclusion – All criteria are met. **Recommendation 39 is rated compliant.**

Recommendation 40 – Other forms of international co-operation[106]

In its 2019 MER, Türkiye was rated largely compliant with R.40. Minor shortcomings included the lack of provisions for the timeliness of responses, some limitations relating to the purposes for which financial supervisors can share information and no specific requirements to prevent the misuse of information. Türkiye is being assessed following changes to R. 40 which now require countries to: ensure that the FIU/competent authority is able to take immediate action, directly or indirectly, to withhold consent for or suspend a transaction; exchange available domestic information for intelligence/investigative purposes and co-operate with foreign counterparts to identify and trace criminal property and property of corresponding value; spontaneously share information on criminal property and property of corresponding value with foreign counterparts without a prior request; and actively support multilateral networks to better facilitate rapid and constructive international co-operation in asset recovery by countries and apply for membership in a relevant ARIN/other body supporting international co-operation.

[106] Recommendation 40 is newly assessed due to changes to the FATF Standards for which Türkiye has not previously been assessed.

General principles

Criterion 40.1

Türkiye's competent authorities can provide international co-operation on ML, predicate offences and TF, upon request. The Financial Intelligence Unit (Financial Crimes Investigation Board-MASAK) is the primary authority for international information exchange in these matters, with its powers explicitly provided under Presidential Decree (PD) No. 1, art. 231(1)(l), 231(1)(m), and 231(5). These powers also extend to the MASAK in its capacity as Supervisor of all FIs, VASPs and DNFBPs (see R. 15, 26 and. 28).

Judicial authorities, LEAs comprising the Turkish National Police, the General Command of the Gendarmerie, the Coast Guard and Customs Enforcement as well as other competent authorities such as the Capital Markets Board (CMB), Insurance and Private Pension Regulation and Supervision Authority (IPRSA), Ministry of Finance and Treasury and the Banking Regulation and Supervision Agency (BRSA) also have statutory authority to exchange information internationally (Banking Law, art. 98). Türkiye's participation in key co-operation mechanisms—including INTERPOL, EUROPOL, EUROJUST and the Basel Committee on Banking Supervision (via BRSA)—enables wide-ranging information exchange.

There are however no specific national legal or other provisions requiring the most rapid response to requests. For FIU, BRSA and CMB, there are no legal impediments regarding the spontaneous sharing of information. s (PD, art. 231 (1) (l) and Guidance for Information Exchange, sec. 3.7; Banking Law, art. 98 and Template MOU; and Capital Market Law (CML), art. 128 (1) (d). Double taxation treaties and the Customs Law, art. 12) also refer.

Criterion 40.2

a) (***Met)*** The MASAK, LEAs, customs and the BRSA have a lawful basis to co-operate internationally (Internal Circular No. 2009/36; Turkish National Police Foreign Relations Department Regulation on Establishment, Duties and Working Regulation 6(1)(a); Europol Agreement with Türkiye; INTERPOL's rules and principles; PD, art 6, 231 (l) and 451 (1) (f); Customs' Agreements and Resolution; Banking Law, art. 98; Insurance Law, art. 29; and CML, art. 128). In line with their powers, MASAK, Turkish National Police (TNP), Customs Enforcement and BRSA have executed MOUs with international partners.

b) There are no legal impediments regarding competent authorities' use of efficient channels.

c) Competent authorities have clear and secure gateways, mechanisms or channels that will facilitate and allow for the transmission and execution of requests. The MASAK uses the Egmont Secure Web; INTERPOL communication mechanism is used by LEAs; and other competent authorities are guided by MoUs which provide channels for information exchange.

d) Competent authorities have clear processes for the prioritisation of requests. In addition to EGMONT requirements, the MASAK has developed an internal Guidance on Exchange of Information with Foreign Counterparts for AML/CFT purposes (July 2021) that sets out, inter alia, which requests require prioritisation and action without delay. For the other competent authorities, INTERPOL principles guide prompt responses and MOUs include prioritisation procedures. However, there were no processes or requirements for any competent authority to execute requests in a timely manner.

e) Competent authorities have clear processes for protecting information received. Officials are prohibited from disclosing information with legal safeguards to protect information received (Banking Law, art. 73; AML Law, art. 22; Insurance Law, art. 31/A; Capital Market Law, art. 135; and Protection of Personal Data Law, art. 9).

Criterion 40.3

The MASAK relies on the Egmont Group membership which allows for the exchange of information between members, and via this arrangement, the MASAK can seek/provide information of its own accord and on behalf of competent authorities. Although not a requirement for MASAK to co-operate, to strengthen the framework, Türkiye has established a wide range of bilateral and multilateral agreements to facilitate international co-operation by its competent authorities. The MASAK concluded 64 bilateral MOUs with foreign FIUs, further enhancing co-operation. The period between the initiation of the proposal and execution varies with each MOU and depends on the foreign counterpart's internal procedures. The Turkish National Police has entered into MoUs with over 100 countries, while Customs has concluded more than 70 bilateral agreements with counterpart agencies. The BRSA, CMB, and IPRSA have also concluded both bilateral MoUs and multilateral arrangements. These include agreements based on the standard frameworks of the Basel Committee on Banking Supervision, IOSCO, and IAIS, covering a broad spectrum of financial supervisory co-operation. The jurisdiction has however not identified which, if any, competent authorities need bilateral or multilateral agreements or arrangements to co-operate and the timelines for the negotiation of any required MoUs, to determine if the agreements (when required) were negotiated and signed in a timely manner.

Criterion 40.4

Türkiye's competent authorities can provide feedback on the use and usefulness of information received from foreign counterparts. While there is no legal obligation mandating the provision of such feedback, there are no legal or operational barriers preventing authorities from doing so. In practice, the MASAK developed a feedback form and incorporated it in the 2021 internal Guidance on Exchange of Information with Foreign Counterparts for AML/CFT Purposes, which supports the delivery of feedback to foreign FIUs.

Criterion 40.5

Türkiye does not impose unreasonable or unduly restrictive conditions on the provision of international co-operation or information exchange regarding the grounds listed in this criterion.

Criterion 40.6

Türkiye has in place general controls and safeguards to ensure that information exchanged by competent authorities is used solely for the purpose for which it was requested or provided. These safeguards are derived from the principles and provisions of international organisations and conventions to which Türkiye is a party, including those that govern confidentiality and the use of shared information. It is a criminal offence for a competent authority to disclose confidential information with breaches resulting in terms of imprisonment (TCL, art. 336). Where necessary, a document shall be assigned a confidentiality level appropriate to the content and judicial or administrative investigations can be initiated against natural or legal persons who violate the security of classified documents or disclose them (Regulation on Procedures and Principles to be applied to classified documents, art. 29, 30). Furthermore, the Civil Servants Law No. 657 (art. 31), prohibits unauthorised disclosure of confidential information and the Personal Data Protection Law No. 6698 (art. 4, 5 and 8), requires that personal data be processed for specific lawful purposes and transferred only where there is a legal basis or authorisation.

Criterion 40.7

Türkiye's competent authorities are subject to confidentiality obligations concerning both the request for co-operation and the information exchanged (See also c. 40.2). These obligations are set out in international co-operation mechanisms and institutional agreements. Authorities such as MASAK, LEAs and financial supervisors (including CMB, IPSRA and BRSA) are bound by confidentiality clauses embedded in MoUs signed with foreign counterparts. These clauses generally reflect the standards of international

frameworks such as the EGMONT Group, INTERPOL, EUROPOL and the IOSCO MMoU, which include detailed provisions on protecting exchanged information (e.g. IOSCO, art. 10–11 and the IAIS, art. 5).

Criterion 40.8

Türkiye's competent authorities are legally empowered to conduct inquiries and exchange information on behalf of their foreign counterparts, to the extent that they could do so in a domestic context. The MASAK, as the main competent authority for ML/TF/PF and main ML/TF/PF supervisor, is authorised under PD No. 1 to perform inquiries and share information with foreign counterparts in relation to ML, predicate offences and TF. The CMB has powers to obtain information necessary for co-operation (Capital Markets Law, art. 89), the IPSRA can engage in co-operation and exchange information within the framework of agreements with the supervisory bodies of foreign countries in matters related to insurance (Insurance Law, art. 29 (2), and the BRSA has authority to exchange information in the context of audits, training and personnel exchange (Banking Law, art. 98.) along with MOUs which allow for the exchange of information. The scope for information exchange is however limited as it refers to "audits, training and personnel" which impedes the widest possible range of information exchange for the BRSA.

Exchange of Information between FIUs

Criterion 40.9

The MASAK has a legal basis to co-operate internationally in matters related to ML, associated predicate offences, and TF. Its authority is established under PD No. 1, art. 231 (l), which explicitly empowers the MASAK to exchange information with foreign counterparts and for this purpose, to sign MoUs in line with its core functions**.**

Criterion 40.10

The MASAK provides feedback to foreign counterparts upon request and, where relevant, on a spontaneous basis. When foreign FIUs request feedback, MASAK informs them of how the information was used and the outcome of the analysis conducted. Furthermore, when the information received plays a significant role in the analysis of a ML or TF case, MASAK also initiates spontaneous feedback to the originating FIU (2021 MASAK Guidance on Exchange of Information with Foreign Counterparts for AML/CFT purposes).

Criterion 40.11

The MASAK has the legal authority to exchange:

(a) all information that it can access or obtain directly or indirectly in accordance with R. 29, and (b) any other information it can access domestically, whether directly or indirectly, in the performance of its duties (Presidential Decree (PD), art. 231 (m). Additionally, the principle of reciprocity is a key element of Türkiye's legal framework governing international information exchange.

Criterion 40.12

Türkiye has established a legal framework that enables the MASAK to take immediate action to suspend transactions suspected of being related to ML, predicate offences, or TF, including upon request from foreign counterparts. The legal framework allows the MASAK to act on suspicious transaction reports, initiate postponement on its own initiative and respond to reasoned foreign requests by referring the matter to the Minister of Treasury and Finance for decision. (Regulation on Postponement of Transactions, art. 4, 5, and 6; and AML Law art. 19 (a)). Upon initiation of a suspension request—whether domestically or from abroad—obliged parties are required to delay execution of the transaction for a defined period, allowing the MASAK time to conduct its analysis and co-ordinate with competent authorities. Article 19/A

in AML law specifically explains that the Ministry of Treasury has the authority to suspend the transactions and this authority can be delegated by the Minister.

Reciprocity is a governing principle in responding to foreign requests, and outcomes are communicated back to the requesting authority. Accordingly, as the MASAK is the primary competent authority for AML/CFT supervision, it can also exchange supervision information. When a request is received from a regulatory or supervisory authority of a country, the MASAK may either take action to respond to the request, or it can convey the request to the relevant competent authority in Türkiye.

Exchange of information between financial supervisors

Criterion 40.13

MASAK, as a supervisory authority on AML/CFT issues, can exchange information within the scope of its duties. In 2021, the MASAK issued a guideline detailing the key factors and priorities for processing such requests which is relevant for the exchange of information between counterparts in terms of AML/CFT. Likewise, other financial supervisory authorities can exchange information subject to reciprocity and non-disclosure restrictions on the condition that reciprocity and equivalent confidentiality protection rules are ensured (see analysis for 40.2 (a)). There are however some legislative provisions which contain limitations regarding the circumstances for which the foreign financial supervisors may use the information (CML art. 98). The BRSA, CMB and Insurance and Private Pension Regulation and Supervision Agency (IPRSA) have concluded MoUs based on the standard frameworks of the Basel Committee on Banking Supervision, IOSCO and IAIS, covering a broad spectrum of financial supervisory co-operation.

Criterion 40.14

Türkiye's financial supervisors are authorised to exchange domestically available information, including that held by FIs, with their foreign counterparts for supervisory purposes. The BRSA is empowered to share information relating to branches of foreign institutions operating in Türkiye, and more broadly, to facilitate audits, training, and personnel exchanges (Banking Law, art. 98) however the provisions do not cover other purposes outside those specified circumstances. Regarding the CMB, provisions broadly empower the supervisory authority to, amongst other things, exchange information and co-operate in any manner with other financial, regulatory and supervisory institutions (CML, art. 128). For the IPRSA, there is the power to engage in all kinds of international co-operation and to enter into agreements to facilitate same (Insurance Law, art. 29 (2).

Criterion 40.15

Türkiye's financial supervisors have varying powers to exchange information relevant for AML/CFT purposes.

(a) Regulatory Information

The MASAK is authorised to exchange regulatory information relevant to its supervisory functions, including information on the AML/CFT regulatory framework. The CMB can exchange general supervisory information with foreign counterparts, including information relating to the inspection of Türkiye-based branches and headquarters (Capital Markets Law, art. 128) (CML). Türkiye's execution of the IOSCO MMoU further supports the exchange of regulatory information within the securities sector. Other supervisors, such as the BRSA and IPRSA, are also empowered to share general information under relevant laws (e.g., Banking Law, art. 98 and Insurance Law, art. 29).

(b) Prudential Information

The BRSA is authorised to exchange prudential information, particularly related to audits and supervision (Banking Law, art. 98) however the provisions do not cover other purposes outside those specified

circumstances. There is also an IOSCO MMoU which further supports the exchange of prudential data in the securities sector. The CMB and IPRSA are similarly able to exchange information on institutional operations and supervisory oversight (CML, art. 128 and Insurance Law, art. 29 respectively). The IAIS Multilateral Memoranda of Understanding (MMoU) also empowers the IPRSA to provide a broad scope of information.

(c) AML/CFT Information

The MASAK, as the FIU and principal AML/CFT supervisory authority, is empowered to exchange AML/CFT information, including information obtained from financial institutions. However, for other financial supervisors, the legal basis for sharing detailed AML/CFT-specific data is not clearly established across all sectors.

Criterion 40.16

Türkiye's financial supervisors demonstrate varying levels of authority to conduct inquiries on behalf of foreign counterparts or to allow foreign authorities to conduct inquiries within Türkiye to facilitate effective group supervision. The MASAK can conduct inquiries on behalf of its foreign counterparts when a request is received from its counterparts (PD 1, art. 231(l) and 231(5). Further, there are legal provisions for the CMB that support international co-operation and information exchange while referencing confidentiality safeguards (CML, art. 128 and 135). However, these Articles, though providing wide-ranging powers, do not explicitly grant the power to conduct inquiries on behalf of foreign counterparts or to facilitate such inquiries directly. Türkiye has referenced relevant international co-operation instruments, including the IOSCO, MoTF (art. 29) and IAIS (MMoUs), which include commitments to cross-border assistance and supervisory co-ordination in the context of group supervision.

The BRSA also operates under the Banking Law (art. 98) as well as bilateral MoUs that contain provisions (e.g., Section V of the draft BRSA MoU) supporting the exchange of information and potentially authorising or facilitating inquiries by foreign supervisors. However, the legal framework itself does not clearly or explicitly set out the authority to conduct inquiries on behalf of or permit direct inquiries by foreign supervisors for the purpose of facilitating effective group-wide supervision.

Criterion 40.17

Türkiye's financial supervisors have, to a large extent, adopted measures, both through legislation and international agreements, to ensure that prior authorisation is obtained before disseminating or using information exchanged with foreign counterparts, unless a legal obligation to disclose exists. For MASAK, confidentiality obligations restrict disclosure of information obtained in the course of duties (AML Law, art. 22). Further, the Turkish Criminal Law (art. 257 and 258) provides sanctions against public officers who misuse their public duty and disclose confidential information in respect of their duties. These provisions do not however include a requirement for the MASAK/or its staff to have the prior authorisation of the requested financial supervisor for dissemination of information.

In the insurance sector, there is a requirement for the IPRSA to seek permission from the originating supervisory authority before sharing any information provided (Regulation on Procedures and Principles on the Monitoring and Supervision of Insurance and Private Pension Sectors, art. 32(4))

In the capital markets sector, confidentiality obligations are imposed (Capital Markets Law, art. 128 and 135). When CMB receives information through MoUs with foreign supervisory authorities, it may use such information for specific activities, for instance, supervisory purposes. Such information may be shared only with prosecution offices, criminal courts and CMB's Board members and staff involved in legal proceedings related to their official duties. There are special rules for exchanges, when the reciprocity principle does not take place in the MoU or where the counterparty is not subject to the obligation of maintaining confidentiality at the same level. There is however no explicit obligation in the CML for the CMB to obtain

prior approval from the requested financial supervisor before disseminating information or using the information for supervisory and non-supervisory purposes. Neither is there a requirement in the CML to inform the requested authority in case there is a legal obligation to disclose information. Nevertheless, the IOSCO MMoU reinforces the requirements for confidentiality (art. 6, 7, 10 and 11). Similarly, there are relevant obligations for the insurance sector (Insurance Law, art. 31/A and the IAIS MMoU, art 4(4) and 5 (6)).

In the banking sector, the BRSA is allowed to exchange information with foreign financial supervisors, which can happen through bilateral MoUs or other arrangements (Banking Law, art. 98). However, there is no explicit obligation in that law for the BRSA to obtain prior approval from the requested financial supervisor before disseminating information or using the information for supervisory and non-supervisory purposes. Further, there is no requirement in the law to inform the requested authority in case there is a legal obligation to disclose information. Notwithstanding, Section VI of the draft BRSA MoU addresses the protection of shared information whereby it requires the requesting authority to notify the BRSA before disclosing any information to domestic third parties. Information sharing is also conditioned on compliance with relevant statutory confidentiality provisions.

Exchange of information between law enforcement authorities

Criterion 40.18

Türkiye's LEAs can exchange domestically available information with their foreign counterparts for both intelligence and investigative purposes related to ML, associated predicate offences and TF. The Turkish National Police (TNP) co-operates with foreign authorities through established international mechanisms such as INTERPOL, EUROPOL and the CARIN network. The Anti-Smuggling and Organised Crime Department (KOM) of the TNP actively uses CARIN for asset tracing, particularly with EU asset recovery offices. Türkiye hosts over 100 foreign liaison officers representing 50 countries and likewise maintains law enforcement counsellors in various countries and international organisations. These in-country and outbound placements support direct, real-time exchanges of intelligence and case-related information.

In addition to operational co-operation, Türkiye has concluded more than 100 bilateral and multilateral agreements and protocols on police co-operation, covering a wide range of crimes, including organised crime, drug trafficking and terrorism. These instruments provide the legal foundation for systematic international information exchange. Further, LEAs may also seek and share financial information with their foreign counterparts. The MASAK, under PD No. 1, is authorised to collect financial intelligence and co-operate with law enforcement, both domestically and internationally, thus facilitating the exchange of financial data in ML/TF investigations.

Criterion 40.19

a) Türkiye's LEAs can exchange domestically available information for intelligence or investigative purposes and to co-operate with foreign counterparts in identifying, tracing, freezing, seizing and confiscating criminal property and property of corresponding value. The TNP exchanges information via INTERPOL, EUROPOL, and through its role as Türkiye's focal point in the CARIN network, particularly through the Anti-Smuggling and Organised Crime Department (TNP-KOM). These channels are used not only for intelligence-sharing but also in preparation for formal mutual legal assistance (MLA) requests, especially regarding asset tracing and recovery efforts.

b) Türkiye's laws authorise public prosecutors to commence investigations upon receiving any credible indication that a criminal offence may have been committed (CPL, art. 160). Further, prosecutors can direct investigations carried out by LEAs (CPL, Art. 161). These provisions apply equally when information is received from foreign counterparts through international co-operation mechanisms**.** The CPL also applies when executing foreign judicial requests (LIJCC, art. 5)

Criterion 40.20

a) LEAs can spontaneously share information with foreign counterparts regarding criminal property and property of corresponding value. Türkiye utilises multiple law enforcement co-operation mechanisms—including INTERPOL, EUROPOL and especially the CARIN network—to engage in proactive exchanges. The TNP-KOM serves as Türkiye's national focal point for CARIN and facilitates information exchange specifically focused on asset tracing and recovery. There is no legal impediment to the spontaneous provision of information in appropriate cases, even where no formal request has been made.

b) Turkish LEAs can identify and trace criminal assets believed to be linked to foreign investigations, when such assets may be located in Türkiye. Through CARIN and other informal networks, LEAs routinely exchange intelligence on property suspected of being the proceeds of crime or otherwise associated with ongoing foreign investigations.

Criterion 40.21

Türkiye's LEAs have the power to conduct inquiries and use available investigative techniques on behalf of foreign counterparts in accordance with domestic law. The TNP is authorised to exchange and act on foreign requests through platforms such as INTERPOL, EUROPOL and the CARIN network, guided by the Internal Circular No. 2009/36. Türkiye signed a co-operation agreement with EUROPOL in 2004, which allows for structured information exchange and operational co-operation.

TNP-KOM, which serves as Türkiye's focal point in the CARIN network, plays a key role in asset tracing and recovery information exchanges, particularly with EU asset recovery offices. Upon receipt of a request through recognised channels such as INTERPOL, EUROPOL, or CARIN, police units are permitted to access domestic law enforcement databases to retrieve relevant information. These exchanges are subject to the operational rules of the respective co-operation mechanism, such as INTERPOL's rules on data processing.

Further, the Directorate General of Customs Enforcement is empowered to co-operate with and international organisations, exchange information, prepare and implement protocols and conduct joint operations. (PD, art. 451 (1) (f)). Additionally, Türkiye refers to the Criminal Procedure Law (CPL) for the application of investigative powers IJCL. This enables special investigative techniques (R.31's analysis refers under the 4th Round) to be used in specific cases when a domestic investigation is initiated by a public prosecutor.

Criterion 40.22

Türkiye's legal and operational framework allows for the formation of joint task teams with foreign counterparts to conduct co-operative investigations. Competent authorities have, by virtue of the ability to exercise a discretion to use special investigative techniques, created joint task teams IJCL art. 1(3)). Public prosecutors may authorise the formation of such teams during the course of an investigation. In practice, Türkiye has formed joint investigation teams, especially in controlled delivery operations. The Ministry of Justice, as the central authority, co-ordinates incoming and outgoing requests in accordance with the IJCL (art. 1(3) and 3). Police co-operation agreements often include provisions on joint investigations and controlled deliveries.

Further legal support is derived from international conventions with direct legal effect under Article 90 of the Constitution, including the Vienna Convention (art. 9), Palermo Convention (art. 19), Merida Convention (art. 49), and the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters. There are no legal impediments to establishing joint task teams in Türkiye.

Criterion 40.23

a) Türkiye participates in multilateral co-operation frameworks that support international asset recovery efforts. There are no legal impediments preventing LEAs from joining such networks or signing MoUs and protocols with foreign counterparts for this purpose.

b) Türkiye is a member of CARIN. The TNP, through its KOM, serves as Türkiye's national focal point in the CARIN. KOM actively exchanges asset recovery-related information with foreign counterparts through this platform.

Exchange of information between non-counterparts

Criterion 40.24

Türkiye has a structured approach to managing requests for information from non-counterpart authorities. Although competent authorities generally cannot and do not exchange information directly with non-counterparts, such diagonal exchanges are facilitated indirectly through the MASAK, which acts as an intermediary. The MASAK routes all such requests to the appropriate counterpart agency, clearly identifying the purpose and originating authority of the request. Regarding the financial supervisors, the IPRSA is permitted to co-operate broadly with foreign supervisory bodies (Regulation on Monitoring and Supervision of the Insurance and Private Pension Sectors, Art. 32(1). The BRSA (Banking Law, art. 98) and CMB (CML, art. 128) also share information within the limits of their authority.

> ***Weighting and conclusion –*** Türkiye's legal and institutional framework for international co-operation is largely consistent with the requirements of Recommendation 40. Competent authorities are able to exchange information with foreign counterparts and co-operate across a wide range of supervisory and enforcement matters. However, certain minor technical shortcomings remain, including the absence of explicit provisions requiring the most rapid response to requests; some legislative constraints on the permissible use of exchanged information by foreign supervisors; and the relatively narrow formulation of the scope of permissible information exchange for the BRSA. These issues do not materially undermine the overall effectiveness of co-operation but warrant refinement to ensure full technical alignment with the Recommendation. **Recommendation 40 is rated largely compliant.**

Annex B. Technical compliance shortcomings

The Recommendations presented in green have been subject to a full assessment, reflecting either amendments to the FATF Standards or substantive changes made by the country to its legal, regulatory, or operational frameworks since its last mutual evaluation. The remaining Recommendations are based on pre-existing information from the country's most recent assessments and have not been reassessed in this review.

Recommendation	Rating*	Factor(s) underlying the rating
1) Assessing risks and applying a risk-based approach	Compliant	• All criteria are met
2) National co-operation and co-ordination	Compliant	• All criteria are met.
3) Money laundering offence	Largely compliant	• The definition of ML is not totally in line with the Conventions as act of concealing and disguising assets requires a specific intention. • The sanctions applied to the legal persons are not fully dissuasive.
4) Confiscation and provisional measures	Largely compliant	• Türkiye's legal framework does not provide for extended confiscation based on a presumption of criminal origin linked to broader criminal activity. (c. 4.8) • Türkiye can use confiscated property to compensate victims of crime in some but not all offences (c.4.13 (b))
5) Terrorist financing offence	Largely compliant	• The sanctions applied to the legal persons are not fully dissuasive (c. 5.8)
6) Targeted financial sanctions related to terrorism and terrorist financing	Largely compliant	• There is no explicit legal requirement that Presidential ratification of listings must take place without delay (c. 6.4) • There is no prohibition against making other related services (to financial services) available to designated persons (c. 6.5) • There are no clear procedures to facilitate review by the 1988 Committee (c. 6.6 (d).
7) Targeted financial sanctions related to proliferation	Partially compliant	• Türkiye does not authorise access to funds or other assets, where countries have determined that the exemption conditions set out in UNSCR 1737 are met, in accordance with the procedures set out therein (c. 7.4). • UNSCR 1737 is not covered in the scope of the RoPF (c. 7.5)
8) Non-profit organisations	Partially compliant	• Türkiye's methodology for identifying the subset of NPOs that within the FATF definition of NPO excludes certain associations based on their share of financial activity, which is not fully in line with the FATF definition of NPOs. (c. 8.1) • Türkiye has not identified the subset of organisations that fall within the FATF definition of NPO (c. 8.3) • Measures to monitor the compliance of NPOs are not risk-based (c. 8.4 (a)) • Due to the "individual criminal responsibility" principle of Türkiye's legal system, criminal sanctions can only be applied to natural persons representing the NPOs (c. 8.4 (b))
9) Financial institutions secrecy laws	Compliant	• All criteria are met.
10) Customer due diligence	Largely compliant	• Lack of requirements for FIs to consider beneficiaries as a risk factor • Lack of explicit reference to all parties to a legal arrangement for conduct of CDD by FIs

		• Requirement to not to open account or terminate business relationship applying only in • case of suspicion relating to customer identification, rather than all relevant CDD • measures
11) Record-keeping	Compliant	• All criteria are met.
12) Politically exposed persons	Compliant	• All criteria are met.
13) Correspondent banking	Compliant	• All criteria are met.
14) Money or value transfer services	Compliant	• All criteria are met.
15) New technologies	Largely compliant	• The minor deficiency in R.35 regarding the existence of an eight-year statute of limitations for administrative fine (Law 5549, art. 13(6)) has a minor impact (c. 15.8 (a)) • The requirement to have risk-based policies and procedures for addressing wire transfers is not fully met (c. 15.9 (b) (iii))
16) Wire transfers	Largely compliant	• Lack of explicit requirements for MVTS providers to consider information on both originator and beneficiary sides to determine whether an STR has to be filed. • Gaps regarding implementation of targeted financial sanctions.
17) Reliance on third parties	Compliant	• All criteria are met.
18) Internal controls and foreign branches and subsidiaries	Largely compliant	• There is no legislative requirement for groups to have policies and procedures for sharing information within groups • No requirements for financial groups to apply additional measures and inform home supervisors if the host country does not permit the proper implementation of AML/CFT measures.
19) Higher-risk countries	Largely compliant	• There is no explicit obligation for financial institutions to apply enhanced due diligence measures for countries when called upon by the FATF, unless such countries are defined as high-risk by the Ministry of Treasury and Finance (c. 19.1)
20) Reporting of suspicious transactions	Compliant	• All criteria are met
21) Tipping-off and confidentiality	Compliant	• All criteria are met
22) DNFBPs: customer due diligence	Largely compliant	• *The deficiencies identified under R.10 for relevant criteria also apply to DNFBPs.(c. 22.1)* •
23) DNFBPs: other measures	Largely compliant	• Deficiencies under R. 19 cascade as DNFBPs are not required to apply EDD to business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF unless such countries are defined as high-risk by the Ministry of Treasury and Finance. (c. 23.3).
24) Transparency and beneficial ownership of legal persons	Largely compliant	• Türkiye has not taken sufficient measures to ensure that the requirements of criteria 24.3(b) and 24.10 are applied by the competent authorities to foreign legal entities posing ML/TF risks and which have sufficient links with Türkiye (c. 24.1) • The risk assessment does not fully address the ML/TF risks of foreign legal persons that have sufficient links to the jurisdiction (c. 24.3) • Türkiye's framework does not ensure that BO information is fully adequate, accurate and up-to-date (c. 24.8) • No information was provided by the jurisdiction to demonstrate that public authorities, including those involved in public procurement or other non-law enforcement competent authorities, have timely access to basic and BO information or that such information is systematically used to verify the identify, ownership or control of legal persons in practice (c. 24.9) • Türkiye's framework relies predominantly on self-declared BO information, with no independent verification and only ad hoc cross-checking mechanisms (c. 24.10) • The sanctions framework has some limitations in being fully effective, proportionate and dissuasive (c. 24.14)
25) Transparency and beneficial	Largely compliant	• The risk assessment of foreign trusts and similar legal arrangements is

ownership of legal arrangements		limited because it focuses primarily on arrangements with a direct and visible presence in Türkiye and does not adequately capture the risks arising from the indirect use of legal arrangements within complex, multi-layered ownership or control structures, thereby constraining its ability to reflect the full spectrum of ML/TF risks.(c. 25.3) • Türkiye's framework does not fully ensure that information on trusts is adequate, accurate and up-to-date, as verification requirement are not sufficiently clear .(c. 25.8) • The sanctions framework has some limitations in being fully effective, proportionate and dissuasive.
26) Regulation and supervision of financial institutions	Compliant	• All criteria are met.
27) Powers of supervisors	Largely compliant	• The amount of financial penalty for failure to comply with AML/CFT requirements not in line with R.35
28) Regulation and supervision of DNFBPs	Largely compliant	• Fit and proper requirements do not extend to associates of criminals from being professionally accredited or holding (or being the beneficial owner of) a significant or controlling interest in a DNFBP (c. 28.4 (b)) • Deficiencies under R. 35 cascade (c. 28.4 (c))
29) Financial intelligence units	Compliant	• All criteria are met.
30) Responsibilities of law enforcement and investigative authorities	Compliant	• All criteria are met.
31) Powers of law enforcement and investigative authorities	Largely compliant	• Competent authorities can use a wide range of investigative techniques and information for ML, TF and some (but not all) associated predicate offenses (c. 31 (2))
32) Cash couriers	Largely compliant	• False disclosure sanctions are not proportionate nor dissuasive unless dealt in the scope of other laws (c. 32.5) • Some shortcoming regarding sanctions for persons carrying out cross border transportations of currency or BNI related to ML/TF offences or predicate offences (c. 32.11)
33) Statistics	Largely compliant	• Statistics maintained by law enforcement authorities are fragmented and not comprehensive (c. 33 (b))
34) Guidance and feedback	Largely compliant	• Scope deficiency: lawyers are not covered. • Full range of competent authorities and SRBs are not involved in the establishment of guidance
35) Sanctions	Largely compliant	• A minor deficiency remains regarding the existence of a statute of limitations.
36) International instruments	Largely compliant	• Some technical gaps with the relevant elements of the conventions.
37) Mutual legal assistance	Compliant	• All criteria are met.
38) Mutual legal assistance: freezing and confiscation	Largely compliant	• There is no legislative obligation to expeditiously respond to requests except as it relates to the Egmont Group. The minor shortcomings in c.3.1 and 3.7 may also slightly limit the range of assistance that can be provided.
39) Extradition	Compliant	• All criteria are met.
40) Other forms of international co-operation	Largely compliant	• The framework does not ensure the most rapid and timely response to international co-operation requests. .(c. 40.1/ c. 40.2) • The jurisdiction has not identified which, if any, competent authorities need bilateral or multilateral agreements or arrangements to co-operate and the timelines for the negotiation of any required MoUs. (c. 40.3) • The BRSA's legal framework does not allow for the widest possible range of information exchange, as its scope is limited to audits, training and personnel exchanges. (c. 40.8) • There are limitations on the purposes for which foreign financial supervisors may use exchanged information, restricting the full scope of co-operation. (c. 40.13) • There is no clear or explicit authorisation for financial supervisors to conduct inquiries on behalf of foreign counterparts or permit direct inquiries to facilitate effective group wide supervision. (c. 40.16) • Provisions do not however include a requirement for MASAK/or its staff to have the prior authorisation of the requested financial supervisor for dissemination of information.(c. 40.17).

Glossary of acronyms

Acronym	Definition
AC	Assessment Commission
AML	Anti-Money Laundering
ATL	Anti-terror Law
BRSA	Banking Regulation and Supervision Agency
BTC	Board of Treasury Controllers
CBCFC	Co-ordination Board for Combating Financial Crimes
CBRT	Central Bank of the Republic of Türkiye
CBT	Credit Bureau of Türkiye
CBF	Cash Declaration Form
CDR	Cash Disclosure Report
CDD	Customer Due Diligence
CMB	Capital Market Board
CPF	Combating Proliferation Financing
CPL	Criminal Procedure Law
CSD	Central Securities Depository
DNFBP	Designated Non-Financial Businesses and Professions
DPMS	Dealers in Precious Metals and Stones
DPRK	Democratic People's Republic of North Korea
EDD	Enhanced Due Diligence
EMIS	Integrated Financial Intelligence System
FI	Financial Institution
FTF	Foreign Terrorist Fighter
GNAT	Grand National Assembly of Türkiye
GGC	Gendarmerie General Command
ISB	Insurance Supervision Board
LEA	Law Enforcement Agencies
MASAK	Financial Crimes Investigation Board (Turkish FIU)
MERSiS	Trade Registry Database
ML	Money Laundering
MLA	Mutual Legal Assistance
MOFA	Ministry of Foreign Affairs
MOI	Ministry of Interior
MoJ	Ministry of Justice
MoT	Ministry of Trade
MOTF	Ministry of Treasury and Finance
MoU	Memorandum of Understanding
MVTS	Money or Value Transfer Services
NICB	National Intelligence Co-ordination Board
NBFI	Non-Banking Financial Institution
NPO	Non-Profit Organisation
NRA	National Risk Assessment
NSC	National Security Council
PD	Presidential Decree
PEP	Politically Exposed Person
PF	Proliferation Financing
PTT	Postal and Telegraph Corporation
RBA	Risk-Based Approach

REA	Real Estate Agent
ROA	Regulation on Association
ROC	Regulation On Program Of Compliance With Obligations Of Anti-Money Laundering And Combating The Financing Of Terrorism
ROF	Regulation on Foundations
ROM	Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism
ROTF	Regulation on the Procedures and Principles Regarding the Implementation of Law on the Prevention of the Financing of Terrorism
STR	Suspicious Transaction Report
SDD	Simplified Due Diligence
TBA	Turkish Banking Association
TCC	Turkish Commercial Code
TCL	Turkish Criminal Law
TCSP	Trust and Company Service Provider
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
TNP	Turkish National Police
TNP TEM	Turkish National Police Counter-Terrorism Department
TRA	Turkish Revenue Authority
TRY	Turkish Lira
TNP (KOM)	Turkish National Police (Anti-Smuggling and Organised Crime Department)
UN	United Nations
UNSCR	UN Security Council Resolution
UYAP	National Judiciary Informatics System



© FATF

www.fatf-gafi.org

September 2026

Mutual Evaluation of Türkiye - Anti-money laundering and countering the financing of terrorism and proliferation financing measures

In this report: a summary of the anti-money laundering (AML)/countering the financing of terrorism (CFT)/counter-proliferation financing (CPF) measures in place in Türkiye at the time of an on-site visit in November 2025.

The report analyses the level of effectiveness of Türkiye's AML/CFT/CPF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how the system could be strengthened.