METHODOLOGY

FOR ASSESSING TECHNICAL COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT/CPF SYSTEMS

ADOPTED IN FEBRUARY 2022

Updated in February 2024

The Methodology in this document is not yet in effect.

This document is for informational purposes only, so that FATF Stakeholders can learn about the expected changes in the FATF's next round of mutual evaluations. The document will come into effect when the FATF commences the fifth round mutual evaluations and may be subject to change before the start of the 5th Round.

Until the FATF completes its 4Th Round of mutual evaluations, the *2013 FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems* and the *Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations* will continue to apply.

For more information about FATF Mutual Evaluations, and the global assessment calendar see:
www.fatf-gafi.org/publications/mutualevaluations

Table of Contents

TABLE OF ACRONYMS

AML/CFT/CPF	Anti-Money Laundering / Countering the Financing of Terrorism / Countering Proliferation Financing (also used for *Combating the financing of terrorism and Combatting the financing of proliferation of weapons of mass destruction*)
BNI	Bearer-Negotiable Instrument
CDD	Customer Due Diligence
CFT	Countering the financing of terrorism
CPF	Countering Proliferation Financing
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IO	Immediate Outcome
IN	Interpretive Note
ML	Money Laundering
MOU	Memorandum of Understanding
MVTS	Money or Value Transfer Service(s)
NPO	Non-Profit Organisation
Palermo Convention	The United Nations Convention against Transnational Organized Crime 2000
PEP	Politically Exposed Person
PF	Proliferation Financing/financing the proliferation of weapons of mass destruction
R.	Recommendation
RBA	Risk-Based Approach
SRB	Self-Regulating Bodies
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
Terrorist Financing Convention	The International Convention for the Suppression of the Financing of Terrorism 1999
TF	Terrorist Financing

UN	United Nations
UNSCR	United Nations Security Council Resolutions
VASP	Virtual Asset Service Provider
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

INTRODUCTION

1. This document provides the basis for undertaking assessments of technical compliance with the FATF Recommendations, as adopted in February 2012 (and updated from time to time), and for reviewing the level of effectiveness of a country's Anti-Money Laundering / Countering the Financing of Terrorism / Countering Proliferation Financing (AML/CFT/CPF) system. It consists of three sections. This first section is an introduction, giving an overview of the assessment Methodology[1], its background, and how it will be used in evaluations/assessments. The second section sets out the criteria for assessing technical compliance with each of the FATF Recommendations. The third section sets out the outcomes, indicators, data and other factors used to assess the effectiveness of the implementation of the FATF Recommendations. The processes and procedures for mutual evaluations are set out in a separate document.

2. For its 5th round of mutual evaluations, the FATF will continue the 4th Round approach of using complementary approaches for assessing technical compliance with the FATF Recommendations, and for assessing whether and how the AML/CFT/CPF system is effective. Therefore, the Methodology comprises two components:

- The technical compliance assessment addresses the specific requirements of the FATF Recommendations, principally as they relate to the relevant legal and institutional framework of the country, and the powers and procedures of the competent authorities. These represent the fundamental building blocks of an AML/CFT/CPF system.
- The effectiveness assessment differs fundamentally from the assessment of technical compliance. It seeks to assess the adequacy of the implementation of the FATF Recommendations, and identifies the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT/CPF system. The focus of the effectiveness assessment is therefore on the extent to which the legal and institutional framework is producing the expected results.

3. Together, the assessments of both technical compliance and effectiveness will present an integrated analysis of the extent to which the country is compliant with the FATF Standards[2] and how successful it is in maintaining a strong AML/CFT/CPF system, as required by those Standards.

4. This Methodology is designed to assist assessors when they are conducting an assessment of a country's compliance with the international AML/CFT/CPF standards. It reflects the requirements set out in the FATF Recommendations and Interpretive Notes, which constitute the international standard to combat money laundering and the financing of terrorism and proliferation, but does not amend or override them. It will assist assessors in identifying the systems and mechanisms developed by countries with diverse legal, regulatory and financial frameworks in order to implement effective

1 The terms "assessment", "evaluation" and their derivatives are used throughout this document, and refer to both mutual evaluations undertaken by the FATF and FSRBs and third-party assessments (i.e. assessments undertaken by the IMF and World Bank).

2 The FATF Standards comprise the FATF Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary.

AML/CFT/CPF systems; and is also useful for countries that are reviewing their own systems, including in relation to technical assistance needs. This Methodology is also informed by the experience of the FATF, the FATF-style regional bodies (FSRBs), the International Monetary Fund and the World Bank in conducting assessments of compliance with earlier versions of the FATF Recommendations.

RISK AND CONTEXT

5. The starting point for every assessment is the assessors' initial understanding of the country's risks and context, in the widest sense, and elements which contribute to them. This includes:

- the nature and extent of the money laundering and terrorist financing risks ;
- the circumstances of the country, which affect the *materiality* of factors that impact different Recommendations (*e.g.,* the makeup of its economy and its financial sector);
- *structural elements* which underpin the AML/CFT/CPF system; and
- *other contextual factors* which could influence the way AML/CFT/CPF measures are implemented and how effective they are.

6. ML/TF *risks* are critically relevant to evaluating technical compliance with Recommendation 1 and the risk-based elements of other Recommendations, and to assess effectiveness. Assessors should consider the nature and extent of the money laundering and terrorist financing risk for the country at the outset of the assessment, and throughout the assessment process. PF risks[3] are also critical to evaluating technical compliance with Recommendation 1. However, assessors should bear in mind that, unlike ML/TF risks, consideration of PF risks is strictly limited to specific elements of the assessment (see the General Interpretation and Guidance for further information specific to Recommendation 1 and financing of proliferation).

7. Assessors should ensure that the risk scoping exercise takes into account the whole range of relevant risk factors, and use the outcome of the risk scoping to guide [and focus] the assessment on the higher risk areas. Examples of relevant factors include the level and type of proceeds-generating crime in the country; the terrorist groups active or raising funds in the country; exposure to cross-border flows of criminal or illicit assets; and the level of significant financial activity in unregulated sectors; and high rates of financial exclusion.[4]

8. Assessors should use the country's own assessment(s) of its risks as an initial basis for understanding the risks, but should not uncritically accept a country's risk assessment as correct, and need not follow all its conclusions. While assessors should always give due consideration to information (e.g., national risk assessment, threat/sectoral/thematic assessment etc.) provided by the assessed country, assessors should also indicate the key sources of credible and reliable

[3] In the context of Recommendation 1, "proliferation financing risk" refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanction obligations referred to in Recommendation 7.

[4] In some cases, financial activity in unregulated sectors and financial exclusion are driven by factors unrelated to ML/TF. Consequently, when taking these factors into account, assessors should also consider the broader context of the country's level of economic development and availability of financial services, its rates of financial inclusion, and the level of risk the country poses to the international financial system.

information which they have relied on to form their views on the reasonableness of the country's assessment. Assessors should also note the guidance in paragraph 21, below on how to evaluate risk assessments in the context of Recommendation 1 and Immediate Outcome 1. There may be cases where assessors cannot conclude that the country's assessment is reasonable, or where the country's assessment is insufficient or non-existent. In such situations, they should consult closely with the national authorities to try to reach a common understanding of what are the key risks within the jurisdiction. If there is no agreement, or if they cannot conclude that the country's assessment is reasonable, then assessors should clearly explain any differences of understanding, and their reasoning on these, in the Mutual Evaluation Report (MER); and should use their understanding of the risks as a basis for assessing the other risk-based elements (e.g., risk-based supervision).

9. Assessors should also consider issues of *materiality*, including, for example, the relative importance of different parts of the financial sector, VASPs and different Designated Non-Financial Businesses and Professions (DNFBPs); the size, integration and make-up of the financial, VASP and DNFBP sectors; the relative importance of different types of financial products or institutions; the amount of business which is domestic or cross-border; the extent to which the economy is cash-based; and estimates of the size of the informal sector and/or shadow economy. Assessors should also be aware of population size, the country's level of development, geographical factors, and trading, cultural and social links. Assessors should consider the relative importance of different sectors and issues in the assessment of both technical compliance and of effectiveness. The most important and relevant issues, including areas of higher ML/TF risks, to the country should be given more weight when determining ratings for technical compliance, and more attention should be given to the most important areas when assessing and rating effectiveness, as set out below.

10. An effective AML/CFT/CPF system normally requires certain *structural elements* to be in place, for example: political stability; a high-level commitment to address AML/CFT issues; stable institutions with accountability, integrity, and transparency; the rule of law; and a capable, independent and efficient judicial system. The examination of structural elements should be informed by factors, including but not limited to, the level of compliance with relevant international obligations[5] and fundamental principles of domestic law[6]. In the AML/CFT context, fundamental principles of domestic law include legal rights such as due process, the presumption of innocence, and a person's right to effective protection by the courts.[7] The lack of such structural elements, or significant weaknesses and shortcomings in the general framework, may significantly hinder the implementation of an effective AML/CFT/CPF framework; and, where assessors identify a lack of

5 Consistent with the *FATF Mandate* and the *FATF Recommendations*, "compliance relevant international obligations" include those of: the United Nations, its Security Council and Committees responsible for issues relevant to the *FATF Mandate*; the Egmont Group of Financial Intelligence Units (see INR.29, para.13); the Basel Committee on Banking Supervision, the International Organization of Securities Commissions, and the International Association of Insurance Supervisors (see INR.40 para.13, footnote 92 and the definition of *core principles* in the Glossary to the FATF Recommendations); and the Council of Europe and the Organization of American States (see R.36).

6 This should be based on information from credible and reliable sources, including the assessed country's most recent MER and FUR, in line with paragraphs 12 and 21 of the *5th Round Methodology*.

7 See the definition of *fundamental principles of domestic law* in the Glossary to the *FATF Recommendations.*

compliance or effectiveness, missing structural elements may be a reason for this and should be identified in the MER, where relevant.

11. *Other contextual factors* that can significantly influence the effectiveness of a country's AML/CFT/CPF measures include the transparency, maturity and sophistication of the criminal justice, regulatory, supervisory and administrative regime in the country; the level of corruption and the impact of measures to combat corruption; or the level of financial exclusion. Such factors can affect the ML/TF risks and increase or reduce the level of compliance or the effectiveness of AML/CFT/CPF measures.

12. Assessors should ensure that contextual factors, including the risks, issues of materiality, structural elements, and other contextual factors are considered to reach a general understanding of the context in which the country's AML/CFT/CPF system operates. These factors should influence which issues assessors consider to be material or higher-risk, and consequently will help assessors determine where to focus their attention in the course of an assessment. Some particularly relevant contextual factors are noted in the context of individual immediate outcomes addressed in the effectiveness component of this Methodology. Assessors should be cautious regarding the information used when considering how these risk and contextual factors might affect a country's evaluation, particularly in cases where they materially affect the conclusions. Assessors should take the country's views into account, but should review them critically, and should also refer to other credible or reliable sources of information (e.g., from international institutions or major authoritative publications), preferably using multiple sources. Assessors should also take into consideration whether the information provided or referred to remains up to date and whether it is of continued relevance. Based on these elements the assessors should make their own judgement of the context in which the country's AML/CFT/CPF system operates, and should make this analysis clear and explicit in the MER.

13. Risk, materiality, and structural or contextual factors may in some cases explain why a country is compliant or non-compliant, or why a country's level of effectiveness is higher or lower than might be expected, on the basis of the country's level of technical compliance. These factors may be an important part of the explanation why the country is performing well or poorly, and an important element of assessors' recommendations about how effectiveness can be improved. Ratings of both technical compliance and effectiveness are judged on a universal standard applied to all countries. An unfavourable context *(e.g.,* where there are missing structural elements), may undermine compliance and effectiveness. However, risks and materiality, and structural or other contextual factors should not be an excuse for poor or uneven implementation of the FATF Standards. Assessors should make clear in the MER which factors they have taken into account; why and how they have done so, and the information sources used when considering them.

SECTOR MATERIALITY AND WEIGHTING

14. In particular, assessors should weight all parts of the financial, DNFBP and VASP sectors in the country as "highly important", "moderately important" or "less important", having regard to risk, materiality and context, and these weightings, and the factors underlying the weighting should be set out in the Mutual Evaluation Report. When assessing the systems and measures in place assessors

should explain how they have weighted the identified strengths and deficiencies of the measures and also explain their impact on the overall sector weighting and assessment.

15. When determining how to weight the various sectors, assessors should consider the ML/TF risks facing each sector and the materiality and the relative importance of each sector, in line with paragraphs 5 to 14 and the Mutual Evaluation Report template (see Annex I of the Methodology). When assessing the materiality of each sector, assessors should take into account, at least, the following factors:

- the size, integration and make-up of the financial, DNFBP and VASP sectors[8];
- the relative importance of different types of financial, DNFBP and VASP products/services or institutions, businesses or professions;
- the maturity of the sector, type of client base, the amount of business which is domestic, regional or international;
- the assessed risks, including the extent to which the economy is based on traceable payment and exchange systems or whether it is cash-based, and whether and to what degree electronic money or other new ways of payment are used; and
- estimates of the size of the informal sector and/or shadow economy

16. Assessors should also take into account structural elements and other contextual factors (e.g. whether established supervisors with sufficient powers, independence, and resources, as well as acknowledged accountability, integrity and transparency are in place for each sector; the robustness of anti-corruption and transparency frameworks and the maturity and sophistication of the regulatory and supervisory regime for each sector)[9].

GENERAL INTERPRETATION AND GUIDANCE

17. A full set of definitions are included in the General Glossary. These definitions are taken from the FATF Recommendations and are published in the Methodology for assessors' convenience. Assessors should also take note of the following guidance on other points of general interpretation, which is important to ensure consistency of approach.

18. **Financial Institutions** – Assessors should have a thorough understanding of the types of entities that engage in the financial activities referred to in the glossary definition of *financial institutions*. It is important to note that such activities may be undertaken by institutions with different generic names (*e.g.,* "bank") in different countries, and that assessors should focus on the activity, not the names attached to the institutions.

19. **VASPs and virtual assets** - Assessors should also have a thorough understanding of the financial institutions, DNFBPs and VASPs that engage in covered activities under the Glossary

8 E.g. including, but not limited to, the business concentration in the different sectors.

9 E.g. special supervisory activities, such as thematic reviews and targeted outreach to specific sectors or institutions.

definition of *virtual asset service provider*. In particular, assessors should note that the requirements of the FATF Standards relating to virtual assets and associated providers are applied by Recommendation 15 ("New Technologies"). INR.15 explicitly confirms that the FATF Definitions of *property, proceeds, funds, funds or other assets* or *other corresponding value* in the Glossary include Virtual Assets. Assessors should bear this in mind when assessing any Recommendations (for technical compliance) or related Immediate Outcomes (for effectiveness) using those terms.[10] See the Note to Assessors in R.15 for more detailed guidance.

20. Assessors should be mindful that countries have flexibility to classify VASPs as a standalone sector or term VASPs as "FIs" or as "DNFBPs." Regardless of how countries may choose to classify VASPs, they should be subject to adequate regulation and risk-based supervision or monitoring by a competent authority, consistent with R.26 and R.27.

21. **Evaluating the country's Assessment of risk** – Assessors are not expected to conduct an independent risk assessment of their own when assessing Recommendation1, Immediate Outcome 1 and core issue 11.2, but on the other hand should not necessarily accept a country's risk assessment as correct. In reviewing the country's risk assessment, assessors should consider the rigour of the processes and procedures employed; and the internal consistency of the assessment (*i.e.* whether the conclusions are reasonable given the information and analysis used). Assessors should focus on high-level issues, not fine details, and should take a common-sense approach to whether the results are reasonable. Where relevant and appropriate, assessors should also consider other credible or reliable sources of information on the country's risks, in order to identify whether there might be any material differences that should be explored further. Where the assessment team considers the country's assessment of the risks to be reasonable the risk-based elements of the Methodology could be considered on the basis of it.

22. **Risk-based requirements** - For each Recommendation where financial institutions, VASPs and DNFBPs should be required to take certain actions, assessors should normally assess compliance on the basis that all financial institutions, VASPs and DNFBPs should have to meet all the specified requirements. However, an important consideration underlying the FATF Recommendations is the degree of risk of money laundering or terrorist financing for particular types of institutions, businesses or professions, or for particular customers, products, transactions, or countries. A country may, therefore, take risk into account in the application of the Recommendations (*e.g.,* in the application of simplified measures), and assessors will need to take the risks, and the flexibility allowed by the risk-based approach, into account when determining whether the measures applied are adequate to mitigate the risks. Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, all such measures must be applied, although the extent of such measures may vary according to the specific level of risk. In this way, the implementation of the risk-based approach relies on the assessment of the full spectrum of risks, from

[10] The terms property, proceeds, funds, funds or other assets and/or corresponding value are used in R.3 (criteria 3.4 and 3.5), R.4 (criteria 4.1, 4.2 and 4.4), R.5 (criteria 5.2, 5.3 and 5.4), R.6 (criteria 6.5, 6.6 and 6.7), R.7 (criteria 7.2, 7.4 and 7.5), R.8 (criteria 8.1 and 8.5), R.10 (criteria 10.7), R.12 (criterion 12.1), R.20 (criterion 20.1), R.29 (criterion 29.4), R.30 (criteria 30.2, 30.3 and 30.5), R.33 (criterion 33.1), R.38 (criteria 38.1, 38.3 and 38.4) and R.40 (criterion 40.17). The words virtual assets need not appear or be explicitly included in legislation referring or defining those terms, provided that there is nothing on the face of the legislation or in case law that would preclude virtual assets from falling within the definition of these terms.

low to high, and, consequentially, on having appropriate mitigating measures[11]. If the scoping exercise or any subsequent phase of the mutual evaluation process identifies unintended consequences such as unduly disrupting or discouraging legitimate NPO activities [12], and this is supported by information from credible and reliable sources[13], the country should demonstrate how its relevant mitigation measures are proportionate and appropriate to the ML/TF risks.

23. **Exemptions for low-risk situations** – Where there is a low risk of money laundering and terrorist financing, countries may decide not to apply some of the Recommendations requiring financial institutions, VASPs and DNFBPs to take certain actions. In such cases, countries should provide assessors with the evidence and analysis which was the basis for the decision not to apply the Recommendations.

24. **Requirements for financial institutions, DNFBPs, VASPs and countries** - The FATF Recommendations state that financial institutions, DNFBPs and VASPs "*should*" or "*should be required to*" take certain actions, or that countries "*should ensure*" that certain actions are taken by financial institutions, DNFBPs, VASPs or other entities or persons. In order to use one consistent phrase, the relevant criteria in this Methodology use the phrase "*Financial institutions should be required*". An equivalent phrase is used for DNFBPs, VASPs or other entities or persons.

25. **Law or enforceable means** – The note on the Legal basis of requirements on financial institutions, DNFBPs and VASPs (at the end of the Interpretive Notes to the FATF Recommendations) sets out the required legal basis for enacting the relevant requirements. For assessors' convenience, this note is included in the Methodology after the General Glossary. Assessors should consider whether the mechanisms used to implement a given requirement qualify as an enforceable means on the basis set out in that note. Assessors should be aware that Recommendations 10, 11, and 20 contain requirements which must be set out in law, while other requirements may be set out in either law or enforceable means. It is possible that types of documents or measures which are not considered to be enforceable means may nevertheless help contribute to effectiveness, and may, therefore, be considered in the context of effectiveness analysis, without counting towards meeting requirements of technical compliance (e.g., voluntary codes of conduct issued by private sector bodies or nonbinding guidance by a supervisory authority).

26. **Assessment for DNFBPs** – Under Recommendations 22, 23 and 28 (and specific elements of Recommendations 6 and 7), DNFBPs and the relevant supervisory (or self-regulatory) bodies are required to take certain actions. Technical compliance with these requirements should only be assessed under these specific Recommendations and should not be carried forward into other

11 The *FATF Recommendations* require countries to understand their (higher and lower) risks, and require financial institutions and DNFBP to take enhanced measures to manage and mitigate higher risks. Correspondingly although it is not required, where the risks are lower, simplified measures may be permitted. Likewise, where there is a proven low risk of ML/TF countries may (but are not obligated to) decide not to apply certain Recommendations to a particular type of financial institution or activity or DNFBP (see INR.1, para.2).

12 This is inconsistent with the *FATF Recommendations* which state that: "Focused measures adopted by countries to protect NPOs from terrorist financing abuse should not disrupt or discourage legitimate charitable activities" (see paragraph 2d of INR.8).

13 As per paragraphs 12 and 21 of the *5th Round Methodology*.

Recommendations relating to financial institutions. However, the assessment of effectiveness should take account of both financial institutions and DNFBPs when examining the relevant outcomes.

27. **Financing of Proliferation** – The requirements of the FATF Standard relating to the financing of proliferation are limited to Recommendation 7 ("Targeted Financial Sanctions"), Recommendation 15 ("New Technologies"), Recommendation 1 ("Assessing Risk and Applying a Risk-based Approach") and Recommendation 2 ("National Co-operation and Co-ordination"). In the context of the effectiveness assessment, all requirements relating to the financing of proliferation are included within Immediate Outcome 11. Issues relating to the financing of proliferation should be considered in those places only, and not in any other parts of the assessment.

28. **National, supra-national and sub-national measures** - In some countries, AML/CFT/ CPF issues are addressed not just at the level of the national government, but also at supra-national, state/province or local levels. When assessments are being conducted, appropriate steps should be taken to ensure that AML/CFT/CPF measures at the state/provincial level are also adequately considered. Equally, assessors should take into account and refer to supra-national measures, including risk assessments, laws or regulations that apply to a country. All relevant measures, at whatever level, should be taken into account both as regards technical compliance and effectiveness. Paragraphs 29 to 32 below and the procedures for conducting assessments explain how to assess any Recommendation and Immediate Outcome in the supra-national context.

29. Countries that are members of supra-national jurisdictions should be assessed individually. Consistent with paragraphs 72-76 of the Methodology, all assessors' recommendations on how to improve the AML/CFT/CPF system should be directed at the assessed country.

30. When assessing the member state of a supra-national jurisdiction, assessors should take into account:

- all relevant laws, regulations and other measures, whether imposed or existing at a supra-national level or imposed as additional measures at the national (or sub-national) level by the assessed Member State of that supra-national jurisdiction according to its national risk;
- how (sub-)national and supra-national AML/CFT/CPF measures complement and interact with each other; and
- any relevant risk assessments at the (sub-)national and supra-national level. For supra-national risk assessments, this includes how the development and conclusions of the risk assessment are informed by the country (e.g. through input or feedback provided by its national agencies), taking into account the guidance in paragraph 21 of the Methodology on evaluating the country's assessment of risk when assessing Recommendation 1, Immediate Outcome 1 and core issue 11.2.

31. Assessing technical compliance in the supra-national context:

- To streamline the process and avoid duplication and inconsistencies, assessment bodies should develop standardised language to describe the elements of the supra-national framework that are common to all member states. This should be done at the start of the 5th round (e.g., in the context of the first assessment(s) member states or as a separate exercise). In case of each assessed country, the standardized language should be modified as appropriate to take into account subsequent changes to the supra-

national framework, any relevant national measures that the individual country has implemented at the domestic level and any differences in implementation.

- Assessors should describe in the Mutual Evaluation Report (in addition to the requirements otherwise laid out in this Methodology):
  - supra-national measures that are directly applicable to the assessed country (e.g. laws and regulations that apply equally to all members states); and
  - whether there are any gaps in the combined framework of national, sub-national and supra-national measures.

32. Assessing effectiveness in the supra-national context (in addition to the requirements otherwise laid out in this Methodology):

(i) Implementation of AML/CFT measures may vary among the member states of a supra-national jurisdiction, depending on the assessed country's particular risk and context, how its national (legal, institutional and operational) framework and other AML/CFT/CPF measures interact with those at the supra-national level, and any gaps in these frameworks or their implementation as against the FATF Standards. Assessors should explore these issues with both the relevant supra-national and the national authorities.

1. When assessing the effectiveness of an Immediate Outcome, assessors should take into account and describe in the MER:
   a the extent to which supra-national measures are implemented in the assessed country;
   b the interplay between implementation of the supra-national and national measures in that area; and
   c how, and the extent to which, AML/CFT/CPF measures at the supra-national level are enforced.

33. **Financial Supervision** – Laws and enforceable means that impose preventive AML/CFT/CPF requirements upon the banking, insurance, and securities sectors should be implemented and enforced through the supervisory process. In these sectors, the relevant core supervisory principles issued by the Basel Committee, IAIS, and IOSCO should also be adhered to – see R.26 footnote 104. For certain issues, these supervisory principles will overlap with or be complementary to the requirements set out in the FATF standards. Assessors should be aware of, and have regard to, any assessments or findings made with respect to the Core Principles, or to other relevant principles or standards issued by the supervisory standard-setting bodies. For other types of financial institutions and VASPs, it will vary from country to country as to how, based on risk, these laws and enforceable means are implemented and enforced, whether through a supervisory or monitoring framework.

34. **Sanctions** – Several Recommendations require countries to have "*effective, proportionate, and dissuasive sanctions*" for failure to comply with AML/CFT requirements. Different elements of these requirements are assessed in the context of technical compliance and of effectiveness. In the technical compliance assessment, assessors should consider whether the country's framework of laws and enforceable means includes a sufficient range of sanctions that they can be applied *proportionately* to

greater or lesser breaches of the requirements[14]. In the effectiveness assessment, assessors should consider whether the sanctions applied in practice are *effective* at ensuring future compliance by the sanctioned institution or person; *proportionate* to the seriousness of the breach or offence; and *dissuasive* of non-compliance by others. Assessors should take into account the country's context and legal system.

35. **International Co-operation** – In this Methodology, international co-operation is assessed in specific Recommendations and Immediate Outcomes (principally Recommendations 36-40 and Immediate Outcome 2). Assessors should also be aware of the impact that a country's ability and willingness to engage in international co-operation may have on other Recommendations and Immediate Outcomes (*e.g.,* on the investigation of crimes with a cross-border element or the supervision of international groups), and set out clearly any instances where compliance or effectiveness is positively or negatively affected by international co-operation.

36. **Draft legislation and proposals** – Assessors should only take into account relevant laws, regulations or other AML/CFT/CPF measures that are in force and effect by the end of the on-site visit to the country. Where bills or other specific proposals to amend the system are made available to assessors, these may be referred to in the report, but should not be taken into account in the conclusions of the assessment or for ratings purposes.

37. **FATF Guidance** - assessors may also consider FATF Guidance as background information on how countries could effectively implement specific requirements. A full list of FATF Guidance is included as an annex to this document. Such guidance may help assessors understand the practicalities of implementing the FATF Recommendations and/or provide examples of mechanisms and practices that contribute to effective implementation, and thus provide background information that could assist assessors in relation to effectiveness. However the guidance should not form part of the assessment.

[14] Examples of types of sanctions include: written warnings; orders to comply with specific instructions (possibly accompanied with daily fines for non-compliance); ordering regular reports from the institution on the measures it is taking; fines for non-compliance; barring individuals from employment within that sector; replacing or restricting the powers of managers, directors, and controlling owners; imposing conservatorship or suspension or withdrawal of the license; or criminal penalties where permitted.

TECHNICAL COMPLIANCE

38. The technical compliance component of the Methodology refers to the implementation of the specific requirements of the FATF Recommendations, including the framework of laws and enforceable means; and the existence, powers and procedures of competent authorities. For the most part, it does not include the specific requirements of the Standards that relate principally to effectiveness. These are assessed separately, through the effectiveness component of the Methodology.

39. The FATF Recommendations, being the recognised international standards, are applicable to all countries. However, assessors should be aware that the legislative, institutional and supervisory framework for AML/CFT/CPF may differ from one country to the next. Provided the FATF Recommendations are complied with, countries are entitled to implement the FATF Standards in a manner consistent with their national legislative and institutional systems, even though the methods by which compliance is achieved may differ. In this regard, assessors should be aware of, and take into account the risks, and the structural or contextual factors for the country.

40. The technical compliance component of the Methodology sets out the specific requirements of each Recommendation as a list of criteria, which represent those elements that should be present in order to demonstrate full compliance with the mandatory elements of the Recommendations. Criteria to be assessed are numbered sequentially for each Recommendation, but the sequence of criteria does not represent any priority or order of importance. In some cases, elaboration (indented below the criteria) is provided in order to assist in identifying important aspects of the assessment of the criteria. For criteria with such elaboration, assessors should review whether each of the elements is present, in order to judge whether the criterion as a whole is met.

COMPLIANCE RATINGS

41. For each Recommendation assessors should reach a conclusion about the extent to which a country complies (or not) with the standard. There are four possible levels of compliance: compliant, largely compliant, partially compliant, and non-compliant. In exceptional circumstances, a Recommendation may also be rated as not applicable. These ratings are based only on the criteria specified in the technical compliance assessment, and are as follows:

Technical compliance ratings		
Compliant	C	There are no shortcomings.
Largely compliant	LC	There are only minor shortcomings.
Partially compliant	PC	There are moderate shortcomings.
Non-compliant	NC	There are major shortcomings.
Not applicable	NA	A requirement does not apply, due to the structural, legal or institutional features of a country.

When deciding on the level of shortcomings for any Recommendation, assessors should consider, having regard to the country context, the number and the relative importance of the criteria met, mostly met, partly met or not met.

42. It is essential to note that it is the responsibility of the assessed country to demonstrate that its AML/CFT/CPF system is compliant with the Recommendations. In determining the level of compliance for each Recommendation, the assessor should not only assess whether laws and enforceable means are compliant with the FATF Recommendations, but should also assess whether the institutional framework is in place.

43. **Weighting of criteria** – The individual criteria used to assess each Recommendation do not all have equal importance, and the number of criteria met is not always an indication of the overall level of compliance with each Recommendation. When deciding on the rating for each Recommendation, assessors should consider the relative importance of the criteria in the context of the country. Assessors should consider how significant any deficiencies are given the country's risk profile and other structural and contextual information (*e.g.,* for a higher risk area or a large part of the financial sector). In some cases, a single deficiency may be sufficiently important to justify an NC rating, even if other criteria are met. Conversely a deficiency in relation to a low risk or little used types of financial activity may have only a minor effect on the overall rating for a Recommendation.

44. **Overlaps between Recommendations** – In many cases the same underlying deficiency will have a cascading effect on the assessment of several different Recommendations.[15] For example: a deficient risk assessment could undermine risk-based measures throughout the AML/CFT system; or a failure to apply AML/CFT regulations to a particular type of financial institution or DNFBP could affect the assessment of all Recommendations which apply to financial institutions or DNFBPs. When considering ratings in such cases, assessors should reflect the deficiency in the factors underlying the rating for each applicable Recommendation, and, if appropriate, mark the rating accordingly. They

15 Assessors are reminded that issues related to PF are assessed exclusively under R.7, IO.11 and specifically identified elements of R.1, R.2, and R.15. Any underlying deficiency related to CPF should not have a cascading effect.

should also clearly indicate in the MER that the same underlying cause is involved in all relevant Recommendations.

EFFECTIVENESS

45. The assessment of the effectiveness of a country's AML/CFT/CPF system is equally as important as the assessment of technical compliance with the FATF standards. Assessing effectiveness is intended to: (a) improve the FATF's focus on outcomes; (b) identify the extent to which the national AML/CFT/CPF system is achieving the objectives of the FATF standards, and identify any systemic weaknesses; and (c) enable countries to prioritise measures to improve their system. For the purposes of this Methodology, effectiveness is defined as "*The extent to which the defined outcomes are achieved*".

46. In the AML/CFT/CPF context, effectiveness is the extent to which financial systems and economies mitigate the risks and threats of money laundering, and financing of terrorism and proliferation. This could be in relation to the intended result of a given (a) policy, law, or enforceable means; (b) programme of law enforcement, supervision, or intelligence activity; or (c) implementation of a specific set of measures to mitigate the money laundering and financing of terrorism risks, and combat the financing of proliferation.

47. The goal of an assessment of effectiveness is to provide an appreciation of the whole of the country's AML/CFT/CPF system and how well it works. Assessing effectiveness is based on a fundamentally different approach to assessing technical compliance with the Recommendations. It does not involve checking whether specific requirements are met, or that all elements of a given Recommendation are in place. Instead, it requires a judgement as to whether, or to what extent defined outcomes are being achieved, *i.e.* whether the key objectives of an AML/CFT/CPF system, in line with the FATF Standards, are being effectively met in practice. The assessment process is reliant on the judgement of assessors, who will work in consultation with the assessed country.

48. It is essential to note that it is the responsibility of the assessed country to demonstrate that its AML/CFT/CPF system is effective. If the evidence is not made available, assessors can only conclude that the system is not effective.

THE FRAMEWORK FOR ASSESSING EFFECTIVENESS

49. For its assessment of effectiveness, the FATF has adopted an approach focusing on a hierarchy of defined outcomes. At the highest level, the objective in implementing AML/CFT/CPF measures is that "*Financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security*". In order to give the right balance between an overall understanding of the effectiveness of a country's AML/CFT/CPF system, and a detailed appreciation of how well its component parts are operating, the FATF assesses effectiveness primarily on the basis of *eleven Immediate Outcomes*. Each of these represents one of the key goals which an effective AML/CFT/CPF system should achieve, and they feed into three Intermediate Outcomes which represent the major thematic goals of AML/CFT/CPF measures. This approach does not seek to assess directly the effectiveness with which a country is implementing individual Recommendations; or the performance of specific organisations, or institutions. Assessors are not expected to evaluate directly the High-Level Objective or Intermediate Outcomes, though these could be relevant when preparing the written MER and summarising the country's overall effectiveness in general terms.

50. The relation between the High-Level Objective, the Intermediate Outcomes, and the Immediate Outcomes, is set out in the diagram* below:

<table>
<tr><td colspan="2">High-Level Objective: Financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security.
(Formatting of this section subject to change)</td></tr>
<tr><td>Intermediate Outcomes:</td><td>Immediate Outcomes:</td></tr>
<tr><td rowspan="2">Policy, co-ordination and co-operation mitigate the money laundering and financing of terrorism risks.</td><td>1. Money laundering and terrorist financing risks are identified, assessed and understood, policies are co-operatively developed and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism.</td></tr>
<tr><td>2. International co-operation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.</td></tr>
<tr><td rowspan="4">Proceeds of crime and funds in support of terrorism are prevented from entering the financial and other sectors or are detected and reported by these sectors.</td><td>3. Supervisors appropriately supervise, monitor and regulate financial institutions and VASPs for compliance with AML/CFT requirements, and financial institutions and VASPs adequately apply AML/CFT preventive measures, and report suspicious transactions. The actions taken by supervisors and by financial institutions and VASPs are commensurate with the risks.</td></tr>
<tr><td>4. Supervisors appropriately supervise, monitor and regulate DNFBPs for compliance with AML/CFT requirements, and DNFBPs adequately apply AML/CFT preventive measures commensurate with the risks, and report suspicious transactions.</td></tr>
<tr><td>5. Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments.</td></tr>
<tr><td>6. Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.</td></tr>
<tr><td rowspan="5">Money laundering threats are detected and disrupted, and criminals are sanctioned and deprived of illicit proceeds. Terrorist financing threats are detected and disrupted, terrorists are deprived of resources, and those who finance terrorism are sanctioned, thereby contributing to the prevention of terrorist acts.</td><td>7. Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.</td></tr>
<tr><td>8. Proceeds and instrumentalities of crime are confiscated</td></tr>
<tr><td>9. Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.</td></tr>
<tr><td>10. Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds.</td></tr>
<tr><td>11. Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.</td></tr>
</table>

This document is shared for information only. The Methodology in this document will apply to the 5th Round of Mutual Evaluations. It is not yet in effect and may be subject to change before the start of the 5th Round.

SCOPING

51. Assessors must assess all eleven of the Immediate Outcomes. However, prior to the on-site visit, assessors should conduct a scoping exercise, in consultation with the assessed country, which should take account of the risks and other factors set out in paragraphs 5 to 16 above. Assessors should, in consultation with the assessed country, identify the higher risk issues, which should be examined in more detail in the course of the assessment and reflected in the final report. They should also seek to identify areas of lower/low risk, which may not need to be examined in the same level of detail. As the assessment continues, assessors should continue to engage the country and review their scoping based on their initial findings about effectiveness, with a view to focusing their attention on the areas where there is greatest scope to improve effectiveness in addressing the key ML/TF risks.

LINKS TO TECHNICAL COMPLIANCE

52. The country's level of technical compliance contributes to the assessment of effectiveness. Assessors should consider the level of technical compliance as part of their scoping exercise. The assessment of technical compliance reviews whether the legal and institutional foundations of an effective AML/CFT/CPF system are present. It is unlikely that a country that is assessed to have a low level of compliance with the technical aspects of the FATF Recommendations will have an effective AML/CFT/CPF system (though it cannot be taken for granted that a technically compliant country will also be effective). In many cases, the main reason for poor effectiveness will be serious deficiencies in implementing the technical elements of the Recommendations.

53. In the course of assessing effectiveness, assessors should also consider the impact of technical compliance with the relevant Recommendations when explaining why the country is (or is not) effective and making recommendations to improve effectiveness. There may in exceptional circumstances be situations in which assessors conclude that there is a low level of technical compliance but nevertheless a certain level of effectiveness (*e.g.,* as a result of specific country circumstances, including low risks or other structural, materiality or contextual factors; particularities of the country's laws and institutions; or if the country applies compensatory AML/CFT/CPF measures which are not required by the FATF Recommendations). Assessors should pay particular attention to such cases in the MER, and must fully justify their decision, explaining in detail the basis and the specific reasons for their conclusions on effectiveness, despite lower levels of technical compliance.

USING THE EFFECTIVENESS METHODOLOGY

54. An assessment of effectiveness should consider each of the eleven Immediate Outcomes individually, but does not directly focus on the Intermediate or High-Level Outcomes. For each of the Immediate Outcomes, there are two overarching questions which assessors should try to answer:

- ***To what extent is the outcome being achieved?*** Assessors should assess whether the country is effective in relation to that outcome (*i.e.* whether the country is achieving the results expected of a well-performing AML/CFT/CPF system (see *Characteristics of an Effective System*)). They should base their conclusions principally on the *core issues*, supported by the *examples of information* and the *examples of specific factors*; and taking

into account the level of technical compliance, risk, materiality and contextual factors.

- ***What can be done to improve effectiveness?*** Assessors should understand the reasons why the country may not have reached a high level of effectiveness and, make recommendations to improve its ability to achieve the specific outcome. They should base their analysis and recommendations on their consideration of the *Characteristics of an Effective System*, the core issue*s* and on the *examples of specific factors that could support the conclusions on core issues*, including activities, processes, resources and infrastructure. They should also consider the effect of technical deficiencies on effectiveness, and the relevance of contextual factors. If assessors are satisfied that the outcome is being achieved to a high degree, they would not need to consider in detail *what can be done to improve effectiveness* (though assessors would be free to identify good practises or potential further improvements, or ongoing efforts needed to sustain a high level of effectiveness).

Characteristics of an Effective System

55. The boxed text at the top of each of the Immediate Outcomes describes the main features and outcomes of an effective system. This sets out the situation in which a country is effective at achieving the outcome, and provides the benchmark for the assessment.

Core Issues to be considered in determining whether the Outcome is being achieved

56. The second section sets out the basis for assessors to judge if, and to what extent, the outcome is being achieved. The *core issues* are the mandatory questions which assessors should seek to answer, in order to get an overview about how effective a country is under each outcome. Assessors' conclusions about how effective a country is should be based on an overview of each outcome, informed by the assessment of the *core issues,* and which takes into account the *Characteristics of an Effective System*.

57. Assessors should examine all the *core issues* listed for each outcome. However, they may vary the degree of detail with which they examine each in order to reflect the degree of risk and materiality associated with that issue in the country. In exceptional circumstances, assessors may also consider additional issues which they consider, in the specific circumstances, to be core to the effectiveness outcome (*e.g.,* alternative measures which reflect the specificities of the country's AML/CFT/CPF system, but which are not included in the *core issues* or as additional *information* or *specific factors*). They should make clear when, and why, any additional issues have been used which are considered to be core.

Examples of information that could support the conclusions on Core Issues

58. The *Examples of Information* sets out the types and sources of information which are most relevant to understanding the extent to which the outcome is achieved, including particular data

points which assessors might look for when assessing the *core issues*. The supporting information and other data can test or validate assessors' understanding of the core issues, and can provide a quantitative element to complete the assessors' picture of how well the outcome is achieved.

59. The supporting information and data listed are not exhaustive and not mandatory. The data, statistics, and other material which are available will vary considerably from country to country, and assessors should make use of whatever information the country can provide in order to assist in reaching their judgement.

60. Assessment of effectiveness is not a statistical exercise. Assessors should use data and statistics, as well as other qualitative information, when reaching an informed judgement about how well the outcome is being achieved, but should interpret the available data critically, in the context of the country's circumstances. The focus should not be on raw data (which can be interpreted in a wide variety of ways and even with contradictory conclusions), but on information and analysis which indicates, in the context of the country being assessed, whether the objective is achieved. Assessors should be particularly cautious about using data relating to other countries as a comparison point in judging effectiveness, given the significant differences in country circumstances, AML/CFT/CPF systems, and data collection practices. Assessors should also be aware that a high level of outputs does not always contribute positively towards achieving the desired outcome.

Examples of specific factors that could support the conclusions on core issues

61. The *factors* section of the Methodology sets out examples of the elements which are normally involved in delivering each outcome. These are not an exhaustive list of the possible factors, but are provided as an aid to assessors when considering the reasons why a country may (or may not) be achieving a particular outcome (*e.g.,* through a breakdown in one of the factors). In most cases, assessors will need to refer to the *factors* in order to reach a firm conclusion about the extent to which a particular outcome is being achieved. It should be noted that the activities and processes listed in this section do not imply a single mandatory model for organising AML/CFT/CPF functions, but only represent the most commonly implemented administrative arrangements, and that the reasons why a country may not be effective are not limited to the factors listed. It should be noted that assessors need to focus on the qualitative aspects of these *factors*, not on the mere underlying process or procedure.

62. Assessors are not required to review all the *factors* in every case. When a country is demonstrably effective in an area, assessors should set out succinctly why this is the case, and highlight any areas of particular good practice, but they do not need to examine every individual factor in this section of the Methodology. There may also be cases in which a country is demonstrably not effective and where the reasons for this are fundamental (*e.g.,* where there are major technical deficiencies). In such cases, there is also no need for assessors to undertake further detailed examination of why the outcome is not being achieved.

63. Assessors should be aware of outcomes which depend on a sequence of different steps, or a *value-chain* to achieve the outcome (*e.g.,* Immediate Outcome 7, which includes investigation, prosecution and sanctioning, in order). In these cases, it is possible that an outcome may not be achieved because of a failure at one stage of the process, even though the other stages are themselves effective.

64. Assessors should also consider contextual factors, which may influence the issues assessors consider to be material or higher risk, and consequently, where they focus their attention. These factors may be an important part of the explanation why the country is performing well or poorly, and an important element of assessors' recommendations about how effectiveness can be improved. However, they should not be an excuse for poor or uneven implementation of the FATF standards.

CROSS-CUTTING ISSUES

65. The Immediate Outcomes are not independent of each other. In many cases an issue considered specifically under one Immediate Outcome will also contribute to the achievement of other outcomes. In particular, the factors assessed under Immediate Outcomes 1 and 2, which consider (a) the country's assessment of risks and implementation of the risk-based approach; and (b) its engagement in international co-operation, may have far-reaching effects on other outcomes (*e.g.,* risk assessment affects the application of risk-based measures under Immediate Outcomes 3 and 4, and the deployment of competent authorities' resources relative to all outcomes; international co-operation includes seeking co-operation to support domestic ML investigations and confiscation proceedings under Immediate Outcomes 7 and 8). Therefore, assessors should take into consideration how their findings for Immediate Outcomes 1 and 2 may have a positive or negative impact on the level of effectiveness for other Immediate Outcomes. These cross-cutting issues are reflected in the *notes to assessors* under each Immediate Outcome.

66. However, where possible, assessors should avoid duplication. Assessors should do so by presenting their analysis of a particular issue once, in what they consider is the most relevant section of the MER, then cross-reference this analysis in other parts of the MER where the issue is relevant. In determining ratings, assessors should give the issue the most weight when rating the IO where they consider the issue is most relevant. The issue may be considered in rating other IOs, but should be given less weight.

CONCLUSIONS ON EFFECTIVENESS

67. For each individual Immediate Outcome, assessors should reach conclusions about the extent to which a country is (or is not) effective. In cases where the country has not reached a high level of effectiveness, assessors should also make recommendations about the reasons why this is the case, and the measures which the country should take to improve its ability to achieve the outcome.

68. ***Effectiveness is assessed in a fundamentally different way to technical compliance***. Assessors' conclusions about the extent to which a country is more or less effective should be based on an overall understanding of the degree to which the country is achieving the outcome. ***The core issues should <u>not</u> be considered as a checklist of criteria***, but as a set of questions which help assessors achieve an appropriate understanding of the country's effectiveness for each of the Immediate Outcomes. The core issues are not equally important, and their significance will vary according to the specific situation of each country, taking into account the ML/TF risks and relevant structural factors. Therefore, assessors need to be flexible and to use their judgement and experience when reaching conclusions. The assessor's conclusions for each Immediate Outcome should clearly explain the weight given to each core issue based on the country's risk, context and materiality and the nature of the core issue.

69. Assessors' conclusions should reflect only *the degree to which the outcome is being achieved*. Assessors should not be unduly influenced by their own national approach. They should also avoid basing their conclusions on the number of problems or deficiencies identified, as it is possible that a country may have several weaknesses which are not material in nature or are offset by strengths in other areas, and is therefore able to achieve a high overall level of effectiveness.

70. ***Assessors' conclusions on the level of effectiveness should be primarily descriptive***. Assessors should set out clearly the extent to which they consider the outcome to be achieved overall, noting any variation, such as particular areas where effectiveness is higher or lower. They should also clearly explain the basis for their judgement, *e.g.,* the deficiencies which they believe are responsible for a lack of effectiveness; the *core issues* and the information which they considered to be most significant; the way in which they understood data and other indicators; and the weight they gave to different aspects of the assessment. Assessors should also identify any areas of particular strength or examples of good practice.

71. In order to ensure clear and comparable decisions, assessors should also summarise their conclusion in the form of a rating. For each Immediate Outcome there are four possible ratings for effectiveness, based on the extent to which the *core issues* and *characteristics* are addressed: *High level of effectiveness; Substantial level of effectiveness; Moderate level of effectiveness; and Low level of effectiveness.* These ratings should be decided on the basis of the following:

Effectiveness ratings	
High level of effectiveness	The Immediate Outcome is achieved to a very large extent. Minor improvements needed.
Substantial level of effectiveness	The Immediate Outcome is achieved to a large extent. Moderate improvements needed.
Moderate level of effectiveness	The Immediate Outcome is achieved to some extent. Major improvements needed.
Low level of effectiveness	The Immediate Outcome is not achieved or achieved to a negligible extent. Fundamental improvements needed.

RECOMMENDATIONS ON HOW TO IMPROVE THE AML/CFT/CPF SYSTEM

72. Assessors' recommendations to a country are a vitally important part of the evaluation. On the basis of their conclusions, assessors should make recommendations of measures that the country should take in order to improve its AML/CFT/CPF system, including both the level of effectiveness and the level of technical compliance. Assessors should determine whether the recommendations are key recommendations for improving effectiveness or technical compliance, and if they are, then these

Key Recommended Actions[16] (KRAs) should be noted separately from other recommendations. There should not normally be more than 2-3 KRAs per Immediate Outcome, including any KRA that concerns a related Recommendation under an Immediate Outcome. Assessors may, in exceptional cases, also set out a limited number of KRAs on contextual factors.[17] The report should prioritise these recommendations for remedial measures, taking into account the country's risks and context its level of effectiveness, and any weaknesses and problems identified. Assessors' recommendations should not simply be to address each of the deficiencies or weaknesses identified, but should add value by identifying and prioritising specific and targeted measures in order to most effectively mitigate the risks the country faces, and the deficiencies that exist, and taking into account relevant contextual factors. This could be on the basis that they offer the greatest and most rapid practical improvements, have the widest-reaching effects, or are easiest to achieve.

73. Assessors should be careful to consider the circumstances and context of the country, and its legal and institutional system when making recommendations, noting that there are several different ways to achieve an effective AML/CFT/CPF system, and that their own preferred model may not be appropriate in the context of the country assessed. Assessors should also consider any structural or contextual factors that impact the level of compliance or effectiveness (see also paragraph 16 above).

74. Assessors should work together with the country to identify the measures needed, so that meaningful recommendations can be made. It is important that the recommendations, and particularly the KRAs, are drafted in a way that is practical, achievable and precise and clear, without being overly prescriptive. They also should be measurable and time-bound, so that the progress achieved can be benchmarked, and be outcome oriented and targeted, so that they result in increased effectiveness.

75. In order to facilitate the development of an action plan by the assessed country, assessors should clearly indicate in their recommendations where a specific action is required, and where there may be some flexibility about how a given priority objective is to be achieved. Assessors should avoid making unnecessarily rigid or overly detailed recommendations (*e.g.,* on the scheduling of certain measures or the prosecution of specific persons), so as not to hinder countries efforts to fully adapt the recommendations to fit local circumstances.

76. Even if a country has a high level of effectiveness, this does not imply that there is no further room for improvement. There may also be a need for action in order to sustain a high level of effectiveness in the face of evolving risks. If assessors are able to identify further actions in areas where there is a high degree of effectiveness, then they should also include these in their recommendations.

16 Key Recommended Actions should only relate to IOs rated ME or LE or Recommendations rated PC or NC where these relate to any IO rated ME or LE. Normally there should be no more than two to three KRA related to each IO, including KRA for technical compliance for Recommendations that relate primarily to that IO. In addition, there may be one KRA for each of Recommendations 3, 5, 6, 10,11, and 20 that is rated NC or PC, where these do not pertain to any IO rated ME or LE.

17 KRAs on contextual factors should be linked to an explanation in the MER setting out the grounds for the recommended action and the intended impact on the country's effective compliance with the FATF standards.

POINT OF REFERENCE

77. If assessors have any doubts about how to apply this Methodology, or about the interpretation of the FATF Standards, they should consult the FATF Secretariat or the Secretariat of their FSRB.

TECHNICAL COMPLIANCE ASSESSMENT

RECOMMENDATION 1 ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH[18]

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, country, designated non-financial businesses and professions; financial institutions, risk, self-regulatory body (SRB), should, supervisors, targeted financial sanctions,* and *terrorist financing (TF).*

OBLIGATIONS AND DECISIONS FOR COUNTRIES

ML/TF risk assessment

1.1 Countries[19] should identify and assess the ML/TF risks for the country,

1.2 Countries should designate an authority or mechanism to co-ordinate actions to assess risks.

1.3 Countries should keep the risk assessments up-to-date.

1.4 Countries should have mechanisms to provide information on the results of the risk assessment(s) to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

PF risk assessment[20]

1.4a Countries[21] should:

a) identify and assess the PF risks for the country;

---

18 The requirements in this recommendation should be assessed taking into account the more specific risk-based requirements in other Recommendations. Under Recommendation 1 assessors should come to an overall view of risk assessment and risk mitigation by countries and financial institutions/DNFBPs as required in other Recommendations, but should not duplicate the detailed assessments of risk-based measures required under other Recommendations. Assessors are not expected to conduct an in-depth review of the country's assessment(s) of risks. Assessors should focus on the process, mechanism, and information sources adopted by the country, as well as the contextual factors, and should consider the reasonableness of the conclusions of the country's assessment(s) of risks.

19 Where appropriate, ML/TF risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

20 In the context of Recommendation 1, "proliferation financing risk" refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.

21 Where appropriate, PF risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

b) designate an authority or mechanism to co-ordinate actions to assess PF risks;

c) keep the PF risk assessments up-to-date; and

d) have mechanisms to provide appropriate information on the results of the PF risk assessment(s) to all relevant competent authorities and SRBs, financial institutions and DNFBPs.

ML/TF risk mitigation

1.5 Based on their understanding of their risks, countries should apply a risk-based approach to allocating resources and implementing measures to prevent or mitigate ML/TF.

1.6 Countries which decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, should demonstrate that:

(a) there is a proven low risk of ML/TF; the exemption occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

(b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is a low risk of ML/TF.

1.7 Where countries identify higher risks, they should ensure that their AML/CFT regime addresses such risks, including through: (a) requiring financial institutions and DNFBPs to take enhanced measures to manage and mitigate the risks; or (b) requiring financial institutions and DNFBPs to ensure that this information is incorporated into their risk assessments.

1.8 Countries may allow simplified measures for some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified, and this is consistent with the country's assessment of its ML/TF risks[22].

1.9 Supervisors and SRBs should ensure that financial institutions and DNFBPs are implementing their obligations under Recommendation 1[23].

PF risk mitigation

1.9a Based on their understanding of their PF risks, countries should implement risk-based measures, commensurate with the risks identified and allocate resources efficiently, to mitigate PF risks, and

[22] Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, countries should ensure that all such measures are applied, although the extent of such measures may vary according to the specific level of risk.

[23] The requirements in this criterion should be assessed taking into account the findings in relation to Recommendations 26 and 28.

(a) countries which decide to exempt financial institutions or DNFBPs from requirements to identify, assess, monitor, manage or mitigate PF risks,[24] should demonstrate that:

(i) the exemption relates to a particular type of financial institution or activity, or DNFBP; and

(ii) there is a proven low risk of PF relating to such financial institutions or activities or DNFBPs;

(b) where countries identify higher risks, they should ensure that their regime to counter PF addresses such risks, including through requiring financial institutions and DNFBPs to take commensurate measures to manage and mitigate the risks;

(c) where countries identify lower risks, they should ensure that the measures applied are commensurate with the level of PF risk, while still ensuring full implementation of targeted financial sanctions as required in Recommendation 7;[25] and

(d) supervisors and SRBs should ensure that financial institutions and DNFBPs are implementing their obligations regarding PF risk under Recommendation 1.

OBLIGATIONS AND DECISIONS FOR FINANCIAL INSTITUTIONS AND DNFBPS

ML/TF risk assessment

1.10 Financial institutions and DNFBPs should be required to take appropriate steps to identify, assess, and understand their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels)[26]. This includes being required to:

(a) document their risk assessments;

(b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) keep these assessments up to date; and

(d) have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs.

24. Regardless of any such exemption, full implementation of targeted financial sanctions as required by Recommendation 7 is mandatory in all cases.

25 The obligations set out in Recommendation 7 place strict requirements on all natural and legal persons, which are not risk-based.

26 The nature and extent of any assessment of ML/TF risks should be appropriate to the nature and size of the business. Competent authorities or SRBs may determine that individual documented risk assessments are not required, provided that the specific risks inherent to the sector are clearly identified and understood, and that individual financial institutions and DNFBPs understand their ML/TF risks.

ML/TF risk mitigation

1.11 Financial institutions and DNFBPs should be required to:

(a) have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified (either by the country or by the financial institution or DNFBP);

(b) monitor the implementation of those controls and to enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

1.12 Countries may only permit financial institutions and DNFBPs to take simplified measures to manage and mitigate risks, if lower risks have been identified, and criteria 1.9 to 1.11 are met. Simplified measures should not be permitted whenever there is a suspicion of ML/TF.

PF risk assessment and mitigation

1.13 Financial institutions and DNFBPs should be required to: [27]

(a) identify and assess, their PF risks[28]. This includes being required to:

(i) document their PF risk assessments;

(ii) keep these assessments up to date; and

(iii) have appropriate mechanisms to provide PF risk assessment information to competent authorities and SRBs;

(b) have policies, controls and procedures, which are approved by senior management and consistent with national requirements and guidance from competent authorities and SRBs, to enable them to manage and mitigate the PF risks that have been identified (either by the country or by the financial institution or DNFBP);

(c) monitor the implementation of those controls and to enhance them if necessary;

(d) take commensurate measures to manage and mitigate the risks where higher PF risks are identified, (i.e. introducing enhanced controls aimed at detecting possible breaches, non-implementation or evasion of targeted financial sanctions under Recommendation 7); and

27 Financial institutions and DNFBPs processes to identify, assess, monitor, manage and mitigate PF risks may be done within the framework of their existing targeted financial sanctions and/or compliance programmes.

28 The nature and extent of any assessment of PF risks should be appropriate to the nature and size of the business. Financial institutions and DNFBP's should always understand their proliferation financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, provided that the specific risks inherent to the sector are clearly identified and understood.

(e) where the PF risks are lower, ensure that measures to manage and mitigate the risks are commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.[29]

[29] Countries should ensure the full implementation of Recommendation 7 in any risk scenario.

RECOMMENDATION 2 NATIONAL CO-OPERATION AND CO-ORDINATION

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, country, risk, should*, and *supervisors.*

2.1 Countries should have national AML/CFT/CPF policies which are informed by the risks[30] identified, and are regularly reviewed.

2.2 Countries should have inter-agency frameworks in place to enable policy makers, the Financial Intelligence Unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities[31] 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.[32]

2.2*bis* To lead such frameworks, countries should designate one or more authorities or have a co-ordination or other mechanism that is responsible for setting national AML/CFT/CPF policies and ensuring co-operation and co-ordination among all relevant agencies.

2.3 Countries should have mechanisms in place to permit effective operational co-operation, and where appropriate, co-ordination and timely sharing of relevant information domestically between different competent authorities, both proactively and on request, for operational purposes related to AML, CFT and CPF.[33]

2.4 Countries should have co-operation and co-ordination between relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).[34]

30 In the context of Recommendation 2, "risk", in relation to PF, refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.

31 Some examples of authorities relevant to such frameworks are listed in INR.2, paragraph 3. When considering these examples, assessors should not consider the list as definitive.

32 There may be a single framework or different frameworks for ML, TF and PF respectively.

33 Some examples of these mechanisms are listed in INR.2, paragraph 4. When considering these examples, assessors should not consider the list as definitive or mandatory.

34 For purposes of technical compliance, the assessment should be limited to whether there is co-operation and, where appropriate, co-ordination, whether formal or informal, between the relevant authorities.

RECOMMENDATION 3 MONEY LAUNDERING OFFENCE

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *country, designated categories of offences, fundamental principles of domestic law, law, legal persons, money laundering offence, property,* and *should*.

3.1 ML should be criminalised on the basis of the Vienna Convention and the Palermo Convention (see Article 3(1)(b)&(c) Vienna Convention and Article 6(1) Palermo Convention)[35].

3.2 The predicate offences for ML should cover all serious offences, with a view to including the widest range of predicate offences. At a minimum, predicate offences should include a range of offences in each of the designated categories of offences.[36]

3.3 Where countries apply a threshold approach or a combined approach that includes a threshold approach,[37] predicate offences should, at a minimum, comprise all offences that:

(a) fall within the category of serious offences under their national law; or

(b) are punishable by a maximum penalty of more than one year's imprisonment; or

(c) are punished by a minimum penalty of more than six months' imprisonment (for countries that have a minimum threshold for offences in their legal system).

3.4 The ML offence should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime.

3.5 When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.

3.6 Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically.

35 Note in particular the physical and material elements of the offence.

36 Recommendation 3 does not require countries to create a separate offence of "participation in an organised criminal group and racketeering". In order to cover this category of "designated offence", it is sufficient if a country meets either of the two options set out in the Palermo Convention, *i.e.* either a separate offence or an offence based on conspiracy.

37 Countries determine the underlying predicate offences for ML by reference to (a) all offences; or (b) to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or (c) to a list of predicate offences; or (d) a combination of these approaches.

3.7 The ML offence should apply to persons who commit the predicate offence, unless this is contrary to fundamental principles of domestic law.

3.8 It should be possible for the intent and knowledge required to prove the ML offence to be inferred from objective factual circumstances.

3.9 Proportionate and dissuasive criminal sanctions should apply to natural persons convicted of ML.

3.10 Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures are without prejudice to the criminal liability of natural persons. All sanctions should be proportionate and dissuasive.

3.11 Unless it is not permitted by fundamental principles of domestic law, there should be appropriate ancillary offences to the ML offence, including: participation in; association with or conspiracy to commit; attempt; aiding and abetting; facilitating; and counselling the commission.

RECOMMENDATION 4 CONFISCATION AND PROVISIONAL MEASURES

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, confiscation, country, freeze, law, property, seize, should, terrorist act,* and *terrorist organisation*.

4.1. Countries should have measures, including legislative measures, that enable the confiscation of the following, whether held by criminal defendants or by third parties:

(a) property laundered;

(b) proceeds of (including income or other benefits derived from such proceeds), or instrumentalities used or intended for use in, ML or predicate offences;

(c) property that is the proceeds of, or used in, or intended or allocated for use in the financing of terrorism, terrorist acts or terrorist organisations; or (d) property of corresponding value.

4.2. Countries should have measures, including legislative measures, that enable their competent authorities to:

(a) identify, trace and evaluate property that is subject to confiscation;

(b) carry out provisional measures, such as freezing or seizing, to prevent any dealing, transfer or disposal of property subject to confiscation;[38]

(c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

4.3. Laws and other measures should provide protection for the rights of *bona fide* third parties.

4.4. Countries should have mechanisms for managing and, when necessary, disposing of property frozen, seized or confiscated.

[38] Measures should allow the initial application to freeze or seize property subject to confiscation to be made *ex-parte* or without prior notice, unless this is inconsistent with fundamental principles of domestic law.

RECOMMENDATION 5 TERRORIST FINANCING OFFENCE

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *country, fundamental principles of domestic law, funds or other assets, law, legal persons, should, terrorist, terrorist act, terrorist financing (TF), terrorist financing offence,* and *terrorist organisation*.

5.1. Countries should criminalise TF on the basis of the Terrorist Financing Convention.[39]

5.2. TF offences should extend to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts).[40]

5.2bis TF offences should include financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

5.3 TF offences should extend to any funds or other assets whether from a legitimate or illegitimate source.

5.4 TF offences should not require that the funds or other assets: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

5.5 It should be possible for the intent and knowledge required to prove the offence to be inferred from objective factual circumstances.

5.6 Proportionate and dissuasive criminal sanctions should apply to natural persons convicted of TF.

5.7 Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be proportionate and dissuasive.

---

39 Criminalisation should be consistent with Article 2 of the International Convention for the Suppression of the Financing of Terrorism.

40 Criminalising TF solely on the basis of aiding and abetting, attempt, or conspiracy is not sufficient to comply with the Recommendation.

5.8 It should also be an offence to:

(a) attempt to commit the TF offence;

(a) participate as an accomplice in a TF offence or attempted offence;

(b) organise or direct others to commit a TF offence or attempted offence; and

(c) contribute to the commission of one or more TF offence(s) or attempted offence(s), by a group of persons acting with a common purpose.[41]

5.9 TF offences should be designated as ML predicate offences.

5.10 TF offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

41 Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a TF offence; or (ii) be made in the knowledge of the intention of the group to commit a TF offence.

RECOMMENDATION 6 TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING

Note to Assessors*:*

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, country, designated non-financial businesses and professions; designated person or entity, designation, ex parte, financial institutions, freeze, funds or other assets, legal persons, should, targeted financial sanctions, terrorist act, terrorist financing (TF), third parties,* and *without delay.*

Identifying and designating

6.1 In relation to designations pursuant to United Nations Security Council 1267/1989 (Al Qaida) and 1988 sanctions regimes (Referred to below as "UN Sanctions Regimes"), countries should:

(a) identify a competent authority or a court as having responsibility for proposing persons or entities to the 1267/1989 Committee for designation; and for proposing persons or entities to the 1988 Committee for designation;

(b) have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in the relevant United Nations Security Council resolutions (UNSCRs);

(c) apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis" when deciding whether or not to make a proposal for designation. Such proposals for designations should not be conditional upon the existence of a criminal proceeding;

(d) follow the procedures and (in the case of UN Sanctions Regimes) standard forms for listing, as adopted by the relevant committee (the 1267/1989 Committee or 1988 Committee); and

(e) provide as much relevant information as possible on the proposed name;[42] a statement of case[43] which contains as much detail as possible on the basis for the

[42] In particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice

[43] This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the relevant committee (the 1267/1989 Committee or 1988 Committee).

listing[44]; and (in the case of proposing names to the 1267/1989 Committee), specify whether their status as a designating state may be made known.

6.2 In relation to designations pursuant to UNSCR 1373, countries should:

(a) identify a competent authority or a court as having responsibility 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.

(b) have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in UNSCR 1373;[45]

(c) when receiving a request, make a prompt determination of whether they are satisfied, according to applicable (supra-) national principles that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373;

(d) apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis" when deciding whether or not to make a designation.[46] Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding; and

(e) when requesting another country to give effect to the actions initiated under the freezing mechanisms, provide as much identifying information, and specific information supporting the designation, as possible.

6.3 The competent authority(ies) should have legal authorities and procedures or mechanisms to:

(a) 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; and

(b) operate *ex parte* against a person or entity who has been identified and whose (proposal for) designation is being considered. *Freezing*

44 Including: specific information supporting a determination that the person or entity meets the relevant designation; the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity

45 This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries pursuant to UNSCR 1373 (2001)

46 A country should apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that "reasonable grounds" or "reasonable basis" exist for a decision to designate a person or entity, and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant country's own motion or at the request of another country.

6.4 Countries should implement targeted financial sanctions without delay.[47]

6.5 Countries should have the legal authority and identify domestic competent authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

(a) Countries should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities.

(b) The obligation to freeze should extend to: (i) all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; (ii) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and (iii) the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as (iv) funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

(c) Countries should prohibit their nationals, or[48] any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or otherwise notified in accordance with the relevant UNSCRs.

(d) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance to financial institutions 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) Countries should require financial institutions and DNFBPs to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

(f) Countries should adopt measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 6.

47 For UNSCR 1373, the obligation to take action without delay is triggered by a designation at the (supra-) national level, as put forward either on the country's own motion or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373.

48 "or", in this particular case means that countries must both prohibit their own nationals and prohibit any persons/entities in their jurisdiction.

De-listing, unfreezing and providing access to frozen funds or other assets

6.6 Countries should have publicly known procedures to de-list and unfreeze the funds or other assets of persons and entities which do not, or no longer, meet the criteria for designation. These should include:

(a) procedures to submit de-listing requests to the relevant UN sanctions Committee in the case of persons and entities designated pursuant to the UN Sanctions Regimes , in the view of the country, do not or no longer meet the criteria for designation. Such procedures and criteria should be in accordance with procedures adopted by the *1267/1989 Committee* or the *1988 Committee*, as appropriate;[49]

(b) legal authorities and procedures or mechanisms to de-list and unfreeze the funds or other assets of persons and entities designated pursuant to UNSCR 1373, that no longer meet the criteria for designation;

(c) with regard to designations pursuant to UNSCR 1373, procedures to allow, upon request, review of the designation decision before a court or other independent competent authority;

(d) with regard to designations pursuant to UNSCR 1988, 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;

(e) with respect to designations on the *Al-Qaida Sanctions List*, procedures for informing designated persons and entities of the availability of the *United Nations Office of the Ombudsperson*, pursuant to UNSCRs 1904, 1989, and 2083 to accept de-listing petitions;

(f) publicly known procedures to unfreeze the 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), upon verification that the person or entity involved is not a designated person or entity; and

(g) mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing guidance to financial institutions 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.

6.7 Countries should authorise access to frozen funds or other assets which 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, in accordance with the

[49] The procedures of the *1267/1989 Committee* are set out in UNSCRs 1730; 1735; 1822; 1904; 1989; 2083 and any successor resolutions. The procedures of the *1988 Committee* are set out in UNSCRs 1730; 1735; 1822; 1904; 1988; 2082; and any successor resolutions.

procedures set out in UNSCR 1452 and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra-)national country pursuant to UNSCR 1373.

RECOMMENDATION 7 TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *accounts, competent authorities, country, designated non-financial businesses and professions; designated person or entity, designation, enforceable means, financial institutions, freeze, funds, funds or other assets, law, legal persons, should, targeted financial sanctions, third parties,* and *without delay*.

7.1 Countries should implement targeted financial sanctions without delay to comply with United Nations Security Council Resolutions, adopted under Chapter VII of the Charter of the United Nations, relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.[50]

7.2 Countries should establish the necessary legal authority and identify competent authorities responsible for implementing and enforcing targeted financial sanctions, and should do so in accordance with the following standards and procedures.

(a) Countries should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities.

(b) The freezing obligation should extend to: (i) all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; (ii) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and (iii) the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as (iv) funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

[50] Recommendation 7 is applicable to all current UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future UNSCRs which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of the FATF Standards to which this Methodology corresponds (June 2017), the UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: UNSCR 1718(2006) on DPRK and its successor resolutions 1874(2009), 2087(2013), 2094(2013), 2270(2016), 2321(2016) and 2356(2017). UNSCR 2231(2015), endorsing the Joint Comprehensive Plan of Action (JCPOA), terminated all provisions of UNSCRs relating to Iran and proliferation financing, including 1737(2006), 1747(2007), 1803(2008) and 1929(2010), but established specific restrictions including targeted financial sanctions. This lifts sanctions as part of a step by step approach with reciprocal commitments endorsed by the Security Council. Implementation day of the JCPOA was on 16 January 2016.

(c) Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant United Nations Security Council Resolutions.

(d) Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance to financial institutions 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) Countries should require financial institutions and DNFBPs to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

(f) Countries should adopt measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 7.

7.3 Countries should adopt measures for monitoring and ensuring compliance by financial institutions and DNFBPs with the relevant laws or enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws or enforceable means should be subject to civil, administrative or criminal sanctions.

7.4 Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities that, in the view of the country, do not or no longer meet the criteria for designation.[51] These should include:

(a) enabling listed persons and entities to petition a request for de-listing at the Focal Point for de-listing established pursuant to UNSCR 1730, or informing designated persons or entities to petition the Focal Point directly;

(b) publicly known procedures to unfreeze the 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), upon verification that the person or entity involved is not a designated person or entity;

(c) authorising access to funds or other assets, where countries have determined that the exemption conditions set out in UNSCRs 1718 and 2231 are met, in accordance with the procedures set out in those resolutions; and

(d) mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing guidance to financial institutions and other persons or entities, including DNFBPs, that may be

[51] In the case of UNSCR 1718 and its successor resolutions, such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the United Nations Security Council pursuant to UNSCR 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution.

holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

7.5 With regard to contracts, agreements or obligations that arose prior to the date on which accounts became subject to targeted financial sanctions:

(a) countries should permit the addition to the accounts frozen pursuant to UNSCRs 1718 or 2231 of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen; and

(b) freezing action taken pursuant to UNSCR 1737 and continued by UNSCR 2231, or taken pursuant to UNSCR 2231 should not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that: (i) the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in UNSCR 2231 and any future successor resolutions; (ii) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity subject to the measures in paragraph 6 of Annex B to UNSCR 2231; and (iii) the relevant countries have submitted prior notification to the Security Council of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.

RECOMMENDATION 8 NON-PROFIT ORGANISATIONS (NPOS)

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *accounts, appropriate authorities, associate NPOs, beneficiaries, competent authorities, country, funds, law, non-profit organisations (NPO), risk, self-regulatory measures, should, terrorist, terrorist financing (TF), terrorist financing abuse*, and *terrorist organisation*.

Assessors should consider, when assessing criteria 8.2 – 8.4 whether the elements apply without unduly disrupting or discouraging legitimate NPO activities.

Taking a risk-based approach

8.1 Since not all organisations working in the not-for-profit realm in a county are inherently high risk [52] without prejudice to the requirements of Recommendation 1, countries should:[53]

(a) identify which subset of organizations fall within the FATF definition[54] of NPO

(b) conduct a risk assessment of these NPOs to identify the nature of TF risks posed to them; and

(c) have in place focused, proportionate and risk-based measures to address the TF risks identified, in line with the risk-based approach.[55]

---

52 NPOs are at varying degrees of risk of TF abuse by virtue of their types, activities or characteristics and the majority may represent low risk.

53 The exercises described under subcriteria 8.1(a) to (c):

a) should use all relevant and reliable sources of information, including through engagement with NPOs;

b) could take a variety of forms and may or may not be a written product; and

c) should be reviewed periodically.

Relevant and reliable sources of information may include, for example, information provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

54 For the purposes of this Recommendation, NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".

55 Countries may consider, where they exist, any self-regulatory measures and related internal control measures in place within NPOs for this requirement.

Note to assessors: Where countries consider self-regulatory measures and related internal control measures in place within NPOs, these measures should be taken into account when considering whether criterion 8.1(c) is satisfied.

Sustained outreach concerning terrorist financing issues[56]

8.2 Countries should:

(a) have clear policies to promote accountability, integrity, and public confidence in the administration and management of NPOs;

(b) undertake outreach and educational programmes as appropriate to raise and deepen awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse;

(c) work with NPOs to develop and refine best practices to address terrorist financing risk and thus protect them from terrorist financing abuse; and

(d) encourage NPOs to conduct transactions via regulated financial and payment channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and areas and the risks of using cash.

Focused, proportionate and risk-based oversight or monitoring of NPOs

8.3 Countries should

(a) take steps to promote focused, proportionte and risk-based oversight or monitoring of NPOs; and

(b) demonstrate that they have in place focused, proportionale and risk-based measures applying to NPOs.[57]

8.4 Appropriate authorities should:

(a) monitor the compliance of NPOs with the the focused, proportionate and risk-based measures being applied to them where needed;[58] and

(b) be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.[59]

Effective information gathering and investigation

---

56 For NPOs identified to be at low risk of TF abuse, countries may focus only on undertaking outreach concerning terrorist financing issues, and may decide to refrain from taking additional mitigating measures

57 Some examples of measures that could be applied to NPOs, in whole or in part, depending on the risks identified are detailed in sub-paragraph 6(b) of INR.8. It is also possible that existing regulatory or other measures may already sufficiently address the current terrorist financing risk to the NPOs in a jurisdiction, although terrorist financing risks to the sector should be periodically re-assessed.

58 In this context, risk-based measures may include self-regulatory measures and related internal control measures in place within NPOs.

59 The range of such sanctions might include freezing of accounts, removal of trustees, fines, de-certification, delicensing and de-registration. This should not preclude parallel civil, administrative or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

8.5 Countries should:

(a) ensure effective co-operation, co-ordination and information-sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs;

(b) have investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations;

(c) ensure that access to relevant information on the administration and management of particular NPOs (including financial and programmatic information) may be obtained during the course of an investigation; and

(d) establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is involved in terrorist financing abuse and/or is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures, or other forms of terrorist support; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, that this information is promptly shared with competent authorities, in order to take preventive or investigative action.

Effective capacity to respond to international requests for information about an NPO of concern

8.6 Countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support.

RECOMMENDATION 9 FINANCIAL INSTITUTION SECRECY LAWS

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *financial institutions, law,* and *should*.

9.1 Financial institution secrecy laws should not inhibit the implementation of the FATF Recommendations.[60]

60 Areas where this may be of particular concern are the ability of competent authorities to access information they require to properly perform their functions in combating ML or FT; the sharing of information between competent authorities, either domestically or internationally; and the sharing of information between financial institutions where this is required by Recommendations 13, 16 or 17.

RECOMMENDATION 10 CUSTOMER DUE DILIGENCE[61] (CDD)

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *accounts, beneficial owner, beneficiary, country, financial institutions, funds, identification data, legal arrangements, legal persons, reasonable measures, risk, satisfied, settlor, should, terrorist financing (TF),* and *trustee*.

10.1 Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

When CDD is required

10.2 Financial institutions should be required to undertake CDD measures when:

(a) establishing business relations;

(b) carrying out occasional transactions above the applicable designated threshold (USD/EUR 15 000), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked;

(c) carrying out occasional transactions that are wire transfers in the circumstances covered by Recommendation 16 and its Interpretive Note;

(d) there is a suspicion of ML/TF, regardless of any exemptions or thresholds that are referred to elsewhere under the FATF Recommendations; or

(e) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Required CDD measures for all customers

10.3 Financial institutions should be required to identify the customer (whether permanent or occasional, and whether natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data).

10.4 Financial institutions should be required to verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person.

10.5 Financial institutions should be required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant

61 The principle that financial institutions conduct CDD should be set out in law, though specific requirements may be set out in enforceable means.

information or data obtained from a reliable source, such that the financial institution is satisfied that it knows who the beneficial owner is.

10.6 Financial institutions should be required to understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship.

10.7 Financial institutions should be required to conduct ongoing due diligence on the business relationship, including:

(a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

(b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

Specific CDD measures required for legal persons and legal arrangements

10.8 For customers that are legal persons or legal arrangements, the financial institution should be required to understand the nature of the customer's business and its ownership and control structure.

10.9 For customers that are legal persons or legal arrangements, the financial institution should be required to identify the customer and verify its identity through the following information:

(a) name, legal form and proof of existence;

(b) the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; and

(c) the address of the registered office and, if different, a principal place of business.

10.10 For customers that are legal persons,[62] the financial institution should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

62 Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

(a) the identity of the natural person(s) (if any[63]) who ultimately has a controlling ownership interest[64] in a legal person; and

(b) to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and

(c) where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

10.11 For customers that are legal arrangements, the financial institution should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries,[65] and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

CDD for Beneficiaries of Life Insurance Policies

10.12 In addition to the CDD measures required for the customer and the beneficial owner, financial institutions should be required to conduct the following CDD measures on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiary is identified or designated:

(a) for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) for a beneficiary that is designated by characteristics or by class or by other means – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the pay-out;

(c) for both the above cases – the verification of the identity of the beneficiary should occur at the time of the pay-out.

63 Ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership.

64 A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%).

65 For beneficiaries of trusts that are designated by characteristics or by class, financial institutions should obtain sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the pay-out or when the beneficiary intends to exercise vested rights.

10.13 Financial institutions should be required to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it should be required to take enhanced measures which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of pay-out.

Timing of verification

10.14 Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers; or (if permitted) may complete verification after the establishment of the business relationship, provided that:

(a) this occurs as soon as reasonably practicable;

(b) this is essential not to interrupt the normal conduct of business; and

(c) the ML/TF risks are effectively managed.

10.15 Financial institutions should be required to adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification.

Existing customers

10.16 Financial institutions should be required to apply CDD requirements to existing customers[66] on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Risk-Based Approach

10.17 Financial institutions should be required to perform enhanced due diligence where the ML/TF risks are higher.

10.18 Financial institutions may only be permitted to apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the financial institution. The simplified measures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.

Failure to satisfactorily complete CDD

10.19 Where a financial institution is unable to comply with relevant CDD measures:

[66] Existing customers as at the date that the new national requirements are brought into force.

(a) it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and

(b) it should be required to consider making a suspicious transaction report (STR) in relation to the customer.

CDD and tipping-off

10.20 In cases where financial institutions form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they should be permitted not to pursue the CDD process, and instead should be required to file an STR.

RECOMMENDATION 11 RECORD KEEPING[67]

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, criminal activity, financial institutions*, and *should*.

11.1 Financial institutions should be required to maintain all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction.

11.2 Financial institutions should be required to keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction.

11.3 Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

11.4 Financial institutions should be required to ensure that all CDD information and transaction records are available swiftly to domestic competent authorities upon appropriate authority.

67 The principle that financial institutions should maintain records on transactions and information obtained through CDD measures should be set out in law.

RECOMMENDATION 12 POLITICALLY EXPOSED PERSONS (PEPS)

Note to Assessors:

Assessors **should** refer to the following Glossary definitions when assessing this Recommendation: *beneficial owner, beneficiary, financial institutions, funds, international organisation, politically exposed persons (PEPs), reasonable measures, risk*, and *should.*

12.1 In relation to foreign PEPs, in addition to performing the CDD measures required under Recommendation 10, financial institutions should be required to:

(a) put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;

(b) obtain senior management approval before establishing (or continuing, for existing customers) such business relationships;

(c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and

(d) conduct enhanced ongoing monitoring on that relationship.

12.2 In relation to domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, in addition to performing the CDD measures required under Recommendation10, financial institutions should be required to:

(a) take reasonable measures to determine whether a customer or the beneficial owner is such a person; and

(b) in cases when there is higher risk business relationship with such a person, adopt the measures in criterion 12.1 (b) to (d).

12.3 Financial institutions should be required to apply the relevant requirements of criteria 12.1 and 12.2 to family members or close associates of all types of PEP.

12.4 In relation to life insurance policies, financial institutions should be required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, financial institutions should be required to inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.

RECOMMENDATION 13 CORRESPONDENT BANKING

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *accounts, correspondent banking, financial institutions, payable-through accounts, shell bank, should,* and *terrorist financing (TF)*.

13.1 In relation to cross-border correspondent banking and other similar relationships, financial institutions should be required to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business, and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action;

(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.

13.2 With respect to "payable-through accounts", financial institutions should be 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; and

(b) is able to provide relevant CDD information upon request to the correspondent bank.

13.3 Financial institutions should be prohibited from entering into, or continuing, correspondent banking relationships with shell banks. They should be required to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks.

RECOMMENDATION 14 MONEY OR VALUE TRANSFER SERVICES (MVTS)

Note to Assessors*:*

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *agent, competent authorities, country, legal persons, money or value transfer service (MVTS),* and *should*.

14.1 Natural or legal persons that provide MVTS (MVTS providers) should be required to be licensed or registered.[68]

14.2. Countries should take action, with a view to identifying natural or legal persons that carry out MVTS without a licence or registration, and applying proportionate and dissuasive sanctions to them.

14.3 MVTS providers should be subject to monitoring for AML/CFT compliance.

14.4 Agents for MVTS providers should be required to be licensed or registered by a competent authority, or the MVTS provider should be required to maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate.

14.5 MVTS providers that use agents should be required to include them in their AML/CFT programmes and monitor them for compliance with these programmes.

[68] Countries need not impose a separate licensing or registration system with respect to licensed or registered financial institutions which are authorised to perform MVTS.

RECOMMENDATION 15 NEW TECHNOLOGIES

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *beneficial owner, beneficiary, competent authorities, country, designated person or entity, financial institutions, foreign counterparts, funds, funds or other assets, law, legal persons, property, risk, should, supervisors, targeted financial sanctions, terrorist financing (TF), trustee, virtual asset*, and *virtual asset service providers (VASPs)*.

For the purposes of applying the FATF Recommendations, countries should consider virtual assets as "property", "proceeds", "funds", "funds or other assets", or other "corresponding value". When assessing any Recommendation(s) using these terms[69], the words "virtual assets" do not have to appear or be explicitly included in legislation referring to or defining those terms.

Assessors should satisfy themselves that the country has demonstrated that nothing in the text of the legislation or in case law precludes virtual assets from falling within the definition of these terms. Where these terms do not cover virtual assets, the deficiency should be noted in the relevant Recommendation(s) that use the term.

Assessors should also satisfy themselves that VASPs may be considered as existing sources of information on beneficial ownership for the purposes of c.24.6(c)(i) and 25.5; and are empowered to obtain relevant information from trustees for the purposes of c.25.3 and 25.4.[70]

Paragraph 1 of INR.15 also requires countries to apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs):

a Where these are preventive measures under Recommendations 10 to 21 and implementation of TFS in R.6 (sub-criteria 6.5(d) and (e), and 6.6(g)) and R.7 (sub-criteria 7.2(d) and (e), criterion 7.3, and sub-criterion 7.4(d)), their application to VASPs should be assessed under Recommendation 15, as should compliance with relevant aspects of R.1, 26, 27, 34, 35 and 37 to 40.

b Where these are other relevant measures relating to virtual assets and VASPs under Recommendations 2 to 5, R.6 (sub-criteria 6.5(a) to (c), 6.6(a) to (f), and criterion 6.7), R.7 (sub-criteria 7.2(a) to (c), 7.4(b) and 7.4(c), and criterion 7.5)), R.8 to 9, and R.29 to 33, their application to virtual assets and VASPs should be assessed in those Recommendations (not in R.15).

Assessors should refer to paragraphs 19-20 of the Introduction section of the Methodology for more guidance on how to assess the FATF Standards relating to virtual assets and VASPs.

---

69 See additional guidance in paragraph 15 of the Introduction to the Methodology.

70 Consideration of VASPs in the context of these criteria is meant to ensure availability of beneficial ownership information. Assessors should not consider these criteria to impose obligations on VASPs.

New technologies

15.1 Countries and financial institutions should identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

15.2 Financial institutions should be required to:

(a) undertake the risk assessments prior to the launch or use of such products, practices and technologies; and

(b) take appropriate measures to manage and mitigate the risks.

Virtual assets and virtual asset service providers.[71]

15.3 In accordance with Recommendation 1, countries should:

(a) identify and assess the money laundering, terrorist financing and proliferation financing risks [72] emerging from virtual asset activities and the activities or operations of VASPs;

(b) based on their understanding of their risks:

(i) apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and

(ii) implement risk-based measures, commensurate with the risks identified and allocate resources efficiently, to mitigate PF risks; and

(c) require VASPs to take appropriate steps to identify, assess, manage and mitigate their money laundering, terrorist financing and proliferation financing risks, as required by criteria 1.10, 1.11 and 1.13.

15.4 Countries should ensure that:

(a) VASPs are required to be licensed or registered[73] at a minimum:[74]

---

71 Note to assessors: Countries that have decided to prohibit virtual assets should only be assessed under criteria 15.1, 15.2, 15.3(a) and 15.3(b), 15.5 and 15.11, as the remaining criteria are not applicable in such cases.

72 "Proliferation financing risk" refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.

73 A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.

74 Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction.

(i) when the VASP is a legal person, in the jurisdiction(s) where it is created;[75] and

(ii) when the VASP is a natural person, in the jurisdiction where its place of business is located[76]; and

(b) competent authorities take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP.

15.5 Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions to them.[77]

15.6 Consistent with the applicable provisions of Recommendations 26 and 27, countries should ensure that:

(a) VASPs are subject to adequate regulation and risk-based supervision or monitoring by a competent authority,[78] including systems for ensuring their compliance with national AML/CFT requirements;

(b) supervisors have adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections, compel the production of information and impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.

15.7 In line with Recommendation 34, competent authorities and supervisors should establish guidelines, and provide feedback, which will assist VASPs in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

15.8 In line with Recommendation 35, countries should ensure that:

(a) there is a range of proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements; and

---

75 References to creating a legal person include incorporation of companies or any other mechanism that is used. To clarify, the requirement in criterion 15.4(a)(i) is that a country must ensure that a VASP created within the country is licenced or registered, but not that any VASP licenced or registered in the country is also registered in any third country where it was created.

76 To clarify, criterion 15.4(a)(ii) requires that a country ensure that a VASP that is a natural person located in their country is licensed or registered in their country; not that any VASP that is a natural person with a place of business located in the country is registered in any third country where it also has a place of business.

77 Note to assessors: Criterion 15.5 applies to all countries, regardless of whether they have chosen to license, register or prohibit virtual assets or VASPs.

78 In this context, a "competent authority" cannot include a SRB.

(b) sanctions should be applicable not only to VASPs, but also to their directors and senior management.

15.9 With respect to the preventive measures, VASPs should be required to comply with the requirements set out in Recommendations 10 to 21, subject to the following qualifications:

(a) R.10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.

(b) R.16 – For virtual asset transfers,[79] countries should ensure that:

(i) originating VASPs obtain and hold required and accurate originator information and required beneficiary information[80] on virtual asset transfers, submit[81] the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities;

(ii) beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities;[82]

(iii) other requirements of R.16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R.16; and

(iv) the same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

15.10 With respect to targeted financial sanctions, countries should ensure that the communication mechanisms, reporting obligations and monitoring referred to in criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d) apply to VASPs.

15.11 Countries should rapidly provide the widest possible range of international co-operation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should have a legal basis for exchanging information with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.[83]

---

79 For the purposes of applying R.16 to VASPs, all virtual asset transfers should be treated as cross-border transfers.

80 As defined in INR.16, paragraph 6, or the equivalent information in a virtual asset context.

81 The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to virtual asset transfers.

82 *Appropriate authorities* means *appropriate competent authorities*, as referred to in paragraph 10 of INR.16.

83 Countries that have prohibited VASPs should fulfil this requirement by having in place a legal basis for permitting their relevant competent authorities (e.g. law enforcement agencies) to exchange information on issues related to VAs and VASPs with non-counterparts, as set out in paragraph 17 of INR.40.

RECOMMENDATION 16 WIRE TRANSFERS

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *accurate, agent, batch transfers, beneficiary, beneficiary financial institution, competent authorities, country, cover payment, cross-border wire transfer, designated person or entity, domestic wire transfers, financial institutions, intermediary financial institution, money or value transfer service (MVTS), originator, ordering financial institution, qualifying wire transfers, reasonable measures, required, risk, serial payment, should, straight-through processing, targeted financial sanctions, unique transaction reference number,* and *wire transfer*.

Ordering financial *institutions*

16.1 Financial institutions should be required to ensure that all cross-border wire transfers of USD/EUR 1 000 or more are always accompanied by the following:

(a) Required and accurate[84] originator information:

(i) the name of the originator;

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and

(iii) the originator's address, or national identity number, or customer identification number, or date and place of birth.

(b) Required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

16.2 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and the financial institution should be required to include the originator's account number or unique transaction reference number.

[84] "Accurate" is used to describe information that has been verified for accuracy; *i.e.* financial institutions should be required to verify the accuracy of the required originator information.

16.3 If countries apply a *de minimis* threshold for the requirements of criterion 16.1, financial institutions should be required to ensure that all cross-border wire transfers below any applicable *de minimis* threshold (no higher than USD/EUR 1 000) are always accompanied by the following:

(a) Required originator information:

(i) the name of the originator; and

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(b) Required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction

16.4 The information mentioned in criterion 16.3 need not be verified for accuracy. However, the financial institution should be required to verify the information pertaining to its customer where there is a suspicion of ML/TF.

16.5 For domestic wire transfers,[85] the ordering financial institution should be required to ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means.

16.6 Where the information accompanying the domestic wire transfer can be made available to the beneficiary financial institution and appropriate authorities by other means, the ordering financial institution need only be required to include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering financial institution should be required to make the information available within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

16.7 The ordering financial institution should be required to maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

16.8 The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above at criteria 16.1-16.7.

[85] This term also refers to any chain of wire transfers that takes place entirely within the borders of the European Union. It is further noted that the European internal market and corresponding legal framework is extended to the members of the European Economic Area.

Intermediary financial institutions

16.9 For cross-border wire transfers, an intermediary financial institution should be required to ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

16.10 Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution should be required to keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary financial institution.

16.11 Intermediary financial institutions should be required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

16.12 Intermediary financial institutions should be required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

Beneficiary financial institutions

16.13 Beneficiary financial institutions should be required to take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

16.14 For cross-border wire transfers of USD/EUR 1 000 or more,[86] a beneficiary financial institution should be required to verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.

16.15 Beneficiary financial institutions should be required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

Money or value transfer service operators

16.16 MVTS providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents.

16.17 In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider should be required to:

[86] Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1 000). Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.

(a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

(b) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

Implementation of Targeted Financial Sanctions

16.18 Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per obligations set out in the relevant UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373, and their successor resolutions.

RECOMMENDATION 17 RELIANCE ON THIRD PARTIES[87]

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *beneficial owner, competent authorities, country, designated non-financial businesses and professions (DNFBP); financial group, financial institutions, identification data, risk, should*, and *third parties*.

17.1 If financial institutions are permitted to rely on third-party financial institutions and DNFBPs to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 (identification of the customer; identification of the beneficial owner; and understanding the nature of the business) or to introduce business, the ultimate responsibility for CDD measures should remain with the financial institution relying on the third party, which should be required to:

(a) obtain immediately the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10;

(b) take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;

(c) satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

17.2 When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

17.3 For financial institutions that rely on a third party that is part of the same financial group, relevant competent authorities[88] may also consider that the requirements of the criteria above are met in the following circumstances:

(a) the group applies CDD and record-keeping requirements, in line with Recommendations 10 to 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18;

(b) the implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority; and

87 This Recommendation does not apply to outsourcing or agency relationships, as set out in paragraph 1 of INR.17.

88 The term *relevant competent authorities* in Recommendation 17 means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities, that should be involved for the branches/subsidiaries.

(c) any higher country risk is adequately mitigated by the group's AML/CFT policies.

RECOMMENDATION 18

INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *country, financial group, financial institutions, law, risk, should*, and *supervisors*.

18.1 Financial institutions should be required to implement programmes against ML/TF, which have regard to the ML/TF risks and the size of the business, and which include the following internal policies, procedures and controls:

(a) compliance management arrangements (including the appointment of a compliance officer at the management level);

(b) screening procedures to ensure high standards when hiring employees;

(c) an ongoing employee training programme; and

(d) an independent audit function to test the system.

18.2 Financial groups should be required to implement group-wide programmes against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group.

These should include the measures set out in criterion 18.1 and also:

(a) policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

(b) the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done).[89] Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management;[90] and

(c) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

89 This could include an STR, its underlying information, or the fact than an STR has been submitted.

90 The scope and extent of the information to be shared in accordance with this criterion may be determined by countries, based on the sensitivity of the information, and its relevance to AML/CFT risk management.

18.3 Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, to the extent that host country laws and regulations permit.

If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups should be required to apply appropriate additional measures to manage the ML/TF risks, and inform their home supervisors.

RECOMMENDATION 19 HIGHER RISK COUNTRIES

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *country, financial institutions, legal persons, risk,* and *should*.

19.1 Financial institutions should be required to apply enhanced due diligence, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

19.2 Countries should be able to apply countermeasures proportionate to the risks: (a) when called upon to do so by the FATF; and (b) independently of any call by the FATF to do so.

19.3 Countries should have measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.

RECOMMENDATION 20 REPORTING OF SUSPICIOUS TRANSACTIONS[91]

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *criminal activity, financial institutions, funds,* and *should*.

20.1 If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity,[92] or are related to TF, it should be required to report promptly its suspicions to the Financial Intelligence Unit.

20.2 Financial institutions should be required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction.

91 The requirement that financial institutions should report suspicious transactions should be set out in law.

92 "Criminal activity" refers to: (a) all criminal acts that would constitute a predicate offence for ML in the country; or (b) at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3.

RECOMMENDATION 21 TIPPING-OFF AND CONFIDENTIALITY

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *criminal activity, financial institutions, law,* and *should*.

21.1 Financial institutions and their directors, officers and employees should be protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU. This protection should be available even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

21.2 Financial institutions and their directors, officers and employees should be prohibited by law from disclosing the fact that an STR or related information is being filed with the Financial Intelligence Unit. These provisions are not intended to inhibit information sharing under Recommendation 18.

RECOMMENDATION 22 DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS (DNFBPS): CUSTOMER DUE DILIGENCE

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *accounts, designated non-financial businesses and professions (DNFBP); express trust, legal persons, nominee shareholder or director, politically exposed persons (PEPs), should,* and *trustee*.

22.1 DNFBPs should be required to comply with the CDD requirements set out in Recommendation 10 in the following situations:

(a) Casinos – when customers engage in financial transactions[93] equal to or above USD/EUR 3 000.

(b) Real estate agents – when they are involved in transactions for a client concerning the buying and selling of real estate.[94]

(c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above USD/EUR 15,000.

(d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for, or carry out, transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creating, operating or management of legal persons or arrangements, and buying and selling of business entities.

(e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the following activities:

93 Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link CDD information for a particular customer to the transactions that the customer conducts in the casino. "Financial transactions" does not refer to gambling transactions that involve only casino chips or tokens.

94 This means that real estate agents should comply with the requirements set out in Recommendation 10 with respect to both the purchasers and the vendors of the property.

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

22.2 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the record-keeping requirements set out in Recommendation 11.

22.3 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the PEPs requirements set out in Recommendation 12.

22.4 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the new technologies' requirements set out in Recommendation 15.

22.5 In the situations set out in Criterion 22.1, DNFBPs should be required to comply with the reliance on third-parties requirements set out in Recommendation 17.

RECOMMENDATION 23 DNFBPS: OTHER MEASURES

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *country, designated non-financial businesses and professions (DNFBP); risk,* and *should*.

When assessing criterion 23.2, assessors should consider whether DNFBPs are required to comply with the internal control requirements set out in criteria 18.1, 18.2 and 18.3.

23.1 The requirements to report suspicious transactions set out in Recommendation 20 should apply to all DNFBPs subject to the following qualifications:

(a) Lawyers, notaries, other independent legal professionals and accountants [95] – when, on behalf of, or for, a client, they engage in a financial transaction in relation to the activities described in criterion 22.1(d).[96]

(b) Dealers in precious metals or stones – when they engage in a cash transaction with a customer equal to or above USD/EUR 15,000.

(c) Trust and company service providers – when, on behalf or for a client, they engage in a transaction in relation to the activities described in criterion 22.1(e).

23.2 In the situations set out in criterion 23.1, DNFBPs should be required to comply with the internal controls requirements set out in Recommendation 18.

23.3 In the situations set out in criterion 23.1, DNFBPs should be required to comply with the higher-risk countries requirements set out in Recommendation 19.

23.4 In the situations set out in criterion 23.1, DNFBPs should be required to comply with the tipping-off and confidentiality requirements set out in Recommendation 21.[97]

---

95 Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings.

96 Where countries allow lawyers, notaries, other independent legal professionals and accountants to send their STRs to their appropriate self-regulatory bodies (SRBs), there should be forms of co-operation between these bodies and the FIU.

97 Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

RECOMMENDATION 24 TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS[98]

Note to Assessors:

1 Assessors should refer to the following Glossary definitions when assessing this Recommendation: *bearer shares and bearer share warrants, beneficial owner, competent authorities, country, designated non-financial businesses and professions (DNFBP); financial institutions, foreign counterparts, law, legal persons, nominator, nominee shareholder or director, reasonable measures, risk, should,* and *terrorist financing (TF)*.

2 If assessors identify a scope deficiency(ies), [99] they should assess this only in criterion 24.1 and not cascade the deficiency(ies) into other criteria that focus on the presence and adequacy of the specific requirements of R.24. When considering how heavily to weight criterion 24.1:

a. individual criteria do not have equal importance and the number of criteria met is not always an indication of the overall compliance with R.24, as per paragraph 43 of the Methodology;

b. the relative importance of a scope deficiency(ies) depends on: i) the materiality of each type of legal person created in the country relative to each other (e.g., based on their number, size and volume of business, types of activities, etc.);[100] ii) the extent to which each type of legal person is covered by the R.24 requirements; and iii) the significance of any scope deficiency(ies), given the

98 Assessors should consider the application of all the criteria to all relevant types of legal persons. The manner in which these requirements are addressed may vary according to the type of legal person involved:

Companies - The measures required by Recommendation 24 are set out with specific reference to companies.

Foundations, Anstalt, and limited liability partnerships - countries should take similar measures and impose similar requirements as those required for companies, taking into account their different forms and structures.

Other types of legal persons - countries should take into account the different forms and structures of those other legal persons, and the levels of ML/TF risks associated with each type of legal person, with a view to achieving appropriate levels of transparency. At a minimum, all legal persons should ensure that similar types of basic information are recorded.

99 There are many types of scope deficiency. One example is if companies are covered by the R.24 requirements, but other forms of legal persons are not (i.e., the country does not impose any R.24 requirements on other forms of legal persons). Another example is if companies are covered by most R.24 requirements, but other forms of legal person are covered by only a few R.24 requirements (i.e., companies and other forms of legal person are covered to varying degrees).

100 This is analogous to how assessors weight the various financial, DNFBP and VASP sectors, as described in paragraphs 9, 14 and 15 of the Methodology.

country's risk profile and other structural and contextual information, including if it is a company formation centre;

c. assessors should explain the basis for their weighting, as a particularly serious scope deficiency(ies) could result in a NC or PC rating even if all other criteria are met, while multiple (but relatively minor) scope deficiencies could result in an LC rating.[101]

3 Sub-criterion 24.1(d) does not require countries to apply measures to individual foreign-created legal persons.

4 The assessment of criterion 24.6 should focus on what requirements and mechanisms a country has implemented in relation to beneficial ownership information, as opposed to criterion 24.8 which should focus on whether the information collected through those mechanisms is adequate, accurate and up-to-date. This means that if assessors note that the relevant information is not adequate, accurate or up-to-date, such deficiencies should be noted under criterion 24.8 (not elsewhere in other criteria).

5 When assessing criteria 24.6, assessors should confirm that the country has in place:

a. the compulsory company approach described in sub-criterion 24.6(a); and

b. a requirement for:

i. a public authority or body to hold beneficial ownership information (a beneficial ownership registry or another body) as described in sub-criterion 24.6(b)(i); or

ii. an alternative mechanism as described in sub-criterion 24.6(b)(ii). If the country has decided to use an alternative mechanism, it should demonstrate that the alternative provides efficient access to BO information;[102] and

c. additional supplementary measures as necessary to ensure the beneficial ownership of a company can be determined.

6 When assessing criteria 24.6(a) and (c), 24.9 and 24.11, assessors should also refer to the fourth paragraph of the *Note to Assessors* for R.15.

101 For example, an NC or PC rating could be justified if companies (which are normally the most materially important type of legal person in any country) are not subject to the basic requirements of R.24, but all other types of legal person are fully covered (depending on the relative material importance and risk of those other types). Conversely, an LC rating could be justified if companies and other types of legal person (which are also materially important in the context of the assessed country) are subject to most of the R.24 requirements, but some other types of legal person (which are not materially important or high risk) are completely outside the scope of R.24.

102 For these purposes, reliance on basic information or existing information (such as the beneficial ownership information obtained and held by financial institutions and DNFBPs pursuant to Recommendations 10 and 22) alone is not sufficient to qualify as an alternative mechanism. However, countries may consider utilising this information to develop an alternative mechanism to ensure efficient access to adequate, accurate and up-to-date beneficial ownership information by competent authorities. Identifying and taking reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official in the circumstances referred to in paragraph 5.b(i.iii) of INR.10 does not constitute collecting *beneficial ownership* information as that term is defined in the Glossary of the FATF Recommendations.

a) Scope extends to companies and other legal persons

24.1 The requirements of Recommendation 24 apply to all forms of legal persons, subject to the following qualifications:

(a) *Companies* – The measures required by Recommendation 24 are set out with specific reference to companies.

(b) *Foundations, Anstalt, Waqf*[103] and limited liability partnerships – Countries should take similar measures and impose similar requirements as those requirements for companies, taking into account their different forms and structures.

(c) *Other types of legal persons* – Countries should take into account the different forms and structures of other legal persons, and the levels of money laundering and terrorist financing risks associated with each type of legal person, with a view to achieving appropriate levels of transparency. At a minimum, countries should ensure that similar types of basic information should be recorded and kept accurate and up-to-date by such legal persons, and that such information is accessible in a timely way by competent authorities.

(d) *Foreign-created legal persons* – Countries should ensure that the requirements of criteria 24.3(b), and 24.10 are applied by the relevant authorities in relation to types of foreign-created legal persons that present ML/TF risks and have sufficient links[104] with the country.

24.2 Countries should have mechanisms that identify, describe and make publicly available the information regarding: (a) the different types, forms and basic features of legal persons in the country; (b) the processes for the creation[105] of legal persons in the country; and (c) the processes for obtaining and recording of basic and beneficial ownership information related to legal persons in the country.

b) Risk assessment and risk mitigation

24.3 Countries should assess the ML/TF risks:

(a) associated with different types of legal persons created in the country, and take appropriate steps to manage and mitigate the risks that they identify. For the other types of legal persons referred to in criterion 24.1c), this means reviewing the money laundering and terrorist financing risks associated with such other types of legal persons, and, based on the level of risk, determine the measures that should

---

103 Except in countries where Waqf are legal arrangements under R.25.

104 Countries may determine what is considered a sufficient link on the basis of risk. Examples of sufficiency tests may include, but are not limited to, when a company has permanent establishment / branch / agency, has significant business activity or has significant and ongoing business relations with financial institutions or DNFBPs, subject to AML/CFT regulation, has significant real estate / other local investment, employs staff, or is a tax resident in the country.

105 References to creating a legal person, include incorporation of companies or any other mechanism that is used.

be taken to ensure that competent authorities have timely access to adequate, accurate and up-to-date beneficial ownership information[106] for such other types of legal persons.

(b) to which their country is exposed, associated with different types of foreign-created legal persons, and take appropriate steps to manage and mitigate the risks that they identify.[107]

c) Basic information

24.4 Countries should require that all companies created in a country are registered in a company registry,[108] which should record and make public all the basic information set out in criterion 24.5(a).

24.5 Countries should require all companies[109] created in their country to obtain and record the following minimum basic information:

(a) company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g., memorandum & articles of association), a list of directors and unique identifier such as a tax identification number[110] or equivalent (where this exists); and

(b) a register of their shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder[111] and categories of shares (including the nature of the associated voting rights).

(c) The company should maintain the basic information set out in criterion 24.5(b) within the country, either at its registered office or at another location notified to the company registry. However, if the company or company registry holds beneficial ownership information within the country, then the register of shareholders need not be in the country, provided that the company can provide this information promptly on request.

106 *Note to assessors:* If assessors note that the relevant information is not "adequate, accurate or up-to-date", such deficiencies should be noted under criterion 24.8 (not elsewhere in other criteria). See also paragraph 4 of the *Note to Assessors* above.

107 This could be done through national and/or supranational measures. These could include requiring beneficial ownership information on some types of foreign-created legal persons to be held as set out under criterion 24.6.

108 Company registry refers to a register in the country of companies incorporated or licensed in that country and normally maintained by or for the incorporating authority. It does not refer to information held by or for the company itself.

109 The information can be recorded by the company itself or by a third person under the company's responsibility.

110 If the unique identifier used is a tax identification number, it should be held by the company registry or another public body.

111 This is applicable to the nominal owner of all registered shares.

d) Beneficial ownership information

24.6 Countries should follow a multi-pronged approach in order to ensure that the beneficial ownership of a company can be determined in a timely manner by a competent authority. This should include the following:

(a) Countries should require companies to obtain and hold adequate, accurate and up-to-date[112] information on the company's own beneficial ownership; to co-operate with competent authorities to the fullest extent possible in determining the beneficial owner, including making the information available to competent authorities in a timely manner; and to co-operate with financial institutions/DNFBPs to provide adequate, accurate and up-to-date information on the company's beneficial ownership information.

(b) Countries should decide, on the basis of risk, context and materiality, what form of registry or alternative mechanisms they will use to enable efficient access to information by competent authorities, and should document their decision. Countries:

i. should require adequate, accurate and up-to-date information [113] on the beneficial ownership of legal persons to be held by a public authority or body[114] (although information need not be held by a single body only);[115] or

ii. may decide to use an alternative mechanism instead of sub-paragraph 24.6(b)(i) if it also provides authorities with efficient access to adequate, accurate and up-to-date beneficial ownership information. For these purposes, reliance on basic information or existing information alone is insufficient, but there must be some specific mechanism that provides efficient access to the information.

iii. Countries should use any additional supplementary measures that are necessary to ensure the beneficial ownership of a company can be determined; including for example information held by regulators or stock exchanges; or

112 *Note to assessors:* If assessors note that the relevant information is not "adequate, accurate or up-to-date", such deficiencies should be noted under criterion 24.8 (not elsewhere in other criteria). See also paragraph 4 of the *Note to Assessors* above.

113 *Note to assessors:* If assessors note that the relevant information is not "adequate, accurate or up-to-date", such deficiencies should be noted under criterion 24.8 (not elsewhere in other criteria). See also paragraph 4 of the *Note to Assessors* above.

114 For example a tax authority, FIU, company registry, or beneficial ownership registry.

115 A body could record beneficial ownership information alongside other information (e.g. basic ownership and incorporation information, tax information), or the source of information could take the form of multiple registries (e.g. for provinces or districts, for sectors, or for specific types of legal person such as NPOs), or of a private body entrusted with this task by the public authority.

information obtained by financial institutions and/or DNFBPs in accordance with Recommendations 10[116] and 22.[117]

24.7 All the persons, authorities and entities mentioned above in criterion 24.6, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company ceases to be a customer of the professional intermediary or the financial institution.

e) Timely access to adequate, accurate and up-to-date information

24.8 Countries should have mechanisms that ensure that basic information and beneficial ownership information, including information provided to the company registry and any available information referred to in criterion 24.6, is adequate,[118] accurate[119] and up to date.[120] [121]

24.9 Competent authorities, and in particular law enforcement authorities and FIUs, should have all the powers necessary to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties, including rapid and efficient access to information held or obtained by a public authority or body or other competent authority

---

116 *Beneficial ownership information* for legal persons is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(i). Controlling shareholders as referred to in, paragraph 5(b)(i) of the interpretive note to Recommendation 10 may be based on a threshold, e.g. any persons owning more than a certain percentage of the company (determined based on the jurisdiction's assessment of risk, with a maximum of 25%). Identifying and taking reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official in the circumstances referred to in paragraph 5.b(i.iii) of INR.10 does not constitute collecting *beneficial ownership* information as that term is defined in the Glossary of the FATF Recommendations.

117 Countries should be able to determine in a timely manner whether a company has or controls an account with a financial institution within the country.

118 *Adequate* information is information that is sufficient to identify the natural person(s) who are the beneficial owner(s), and the means and mechanisms through which they exercise beneficial ownership or control. Examples of information aimed at identifying the natural person(s) who are the beneficial owner(s) include the full name, nationality(ies), the full date and place of birth, residential address, national identification number and document type, and the tax identification number or equivalent in the country of residence.

119 *Accurate* information is information, which has been verified to confirm its accuracy by verifying the identity and status of the beneficial owner using reliable, independently sourced/obtained documents, data or information. The extent of verification measures may vary according to the specific level of risk. Countries should consider complementary measures as necessary to support the accuracy of beneficial ownership information, e.g. discrepancy reporting

120 *Up-to-date* information is information which is as current and up-to-date as possible, and is updated within a reasonable period (e.g. within one month) following any change.

121 *Note to assessors:* If assessors note that the relevant information is not "adequate, accurate or up-to-date", such deficiencies should be noted under criterion 24.8 (not elsewhere in other criteria). See also paragraph 4 of the *Note to Assessors* above.

on basic and beneficial ownership information, and/or on the financial institutions or DNFBPs which hold this information. In addition, countries should ensure public authorities at national level and others as appropriate have timely access to basic and beneficial ownership information on legal persons in the course of public procurement.

24.10 Countries should have a combination of mechanisms to achieve the objective of enabling the competent authorities to obtain, or have access in a timely fashion to, adequate, accurate and up-to-date information[122] on the beneficial ownership and control of foreign-created companies and other legal persons that present ML/TF risks and have a sufficient link with the country.[123]

24.11 Countries should require their company registry to facilitate timely access by financial institutions, DNFBPs and other countries' competent authorities to the public information they hold, and, at a minimum to the information referred to in criterion 24.5(a) above.

f) Obstacles to transparency

24.12 Countries should take measures to prevent and mitigate the risk of the misuse of bearer shares and bearer share warrants (or any other similar instruments without traceability) by:

(a) prohibiting the issuance of new bearer shares and bearer share warrants; and

(b) for any existing bearer shares and bearer share warrants, applying one or more of the following mechanisms within a reasonable timeframe:[124]

i. converting them into a registered form;

ii. immobilizing them by requiring them to be held with a regulated financial institution or professional intermediary, with timely access to the information by the competent authorities; and

iii. during the period before (i) or (ii) is completed, requiring holders of bearer instruments to notify the company, and the company to record their identity before any rights associated therewith can be exercised.

24.13 Countries should take measures to prevent and mitigate the risk of the misuse of nominee shareholding and nominee directors, by applying one or more of the following mechanisms:

a) requiring nominee shareholders and directors to disclose their nominee status and the identity of their nominator to the company and to any relevant registry, and for

122 Ibid.

123 Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements of criteria 24.3(b).

124 These requirements do not apply to newly issued and existing bearer shares or bearer share warrants of a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership.

this information to be included in the relevant register, and for the information to be obtained, held or recorded by the public authority or body or the alternative mechanism referred to in criterion 24.6. Nominee status should be included in public information;

b) requiring nominee shareholders and directors to be licensed,[125] for their nominee status and the identity of their nominator to be obtained, held or recorded by the public authority or body or alternative mechanism referred to in criterion 24.6 and for them to maintain information identifying their nominator and the natural person on whose behalf the nominee is ultimately acting, [126] and make this information available to the competent authorities upon request;[127] or

c) enforcing a prohibition of the use of nominee shareholders or nominee directors.

g) Liability and sanctions

24.14 There should be a clearly stated responsibility to comply with the requirements in the interpretive note to Recommendation 24, as well as liability and proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to properly comply with the requirements.

h) International cooperation

24.15 Countries should rapidly, constructively and effectively provide the widest possible range of international cooperation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40, which includes:

a) not placing unduly restrictive conditions on the exchange of information or assistance e.g., refuse a request on the grounds that it involves a fiscal (including tax) matters, bank secrecy, etc.;

b) facilitating access by foreign competent authorities to basic information held by company registries;

c) exchanging information on shareholders;

d) using their powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts;

---

125 A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions or DNFBPs (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform nominee activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.

126 Identifying the beneficial owner in situations where a nominee holds a controlling interest or otherwise exercises effective control requires establishing the identity of the natural person on whose behalf the nominee is ultimately, directly or indirectly, acting.

127 For intermediaries involved in such nominee activities, reference should be made to R.22 and R.28 in fulfilling the relevant requirements.

e) monitoring the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad;

f) keeping in a readily accessible manner information held or obtained for the purpose of identifying beneficial ownership; and

g) designating and making publicly known the agency(ies) responsible for responding to all international requests for beneficial ownership information.

RECOMMENDATION 25 TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS

Note to Assessors:

1 Assessors should refer to the following Glossary definitions when assessing this Recommendation: *beneficial owner, beneficiary, competent authorities, country, designated non-financial businesses and professions (DNFBP), enforceable means, express trust, financial institutions, foreign counterparts, law, legal arrangements, legal persons, property, risk, settlor, should, terrorist financing,* and *trustee.*

2 If assessors identify a scope deficiency(ies),[128] they should assess this only in criterion 25.1 and not cascade the deficiency(ies) into other criteria that focus on the presence and adequacy of the specific requirements of R.25. When considering how heavily to weight criterion 25.1:

   a. individual criteria do not have equal importance and the number of criteria met is not always an indication of the overall compliance with R.25, as per paragraph 43 of the Methodology;

   b. the relative importance of a scope deficiency(ies) depends on: i) the materiality of each type of legal arrangement set up administered or whose trustees or persons holding an equivalent position in a similar legal arrangement are resident in the country relative to each other (e.g., based on their number, size and volume of business, types of activities, etc.);[129] ii) the extent to which each type of legal arrangement is covered by the R.25 requirements; and iii) the significance of any scope deficiency(ies), given the country's risk profile and other structural and contextual information, including if it is a trust formation centre;

   c. assessors should explain the basis for their weighting, as a particularly serious scope deficiency(ies) could result in a NC or PC rating even if all other criteria are met, while multiple (but relatively minor) scope deficiencies could result in an LC rating.[130]

3 The assessment of criterion 25.4 should focus on what requirements a country has

[128] There are many types of scope deficiency. The following examples assume the assessed country has express trusts governed under their law. One example is if trusts are covered by the R.25 requirements, but other forms of legal arrangements are not. Another example is if trusts are covered by most R.25 requirements, while other types of legal arrangements are covered by only a few R.25 requirements (i.e., trusts and other forms of legal arrangements are covered to varying degrees).

[129] This is analogous to how assessors weight the various financial, DNFBP and VASP sectors, as described in paragraphs 9, 14 and 15 of the Methodology.

[130] For example, an NC or PC rating could be justified if the country is a trust formation centre that does not apply the basic requirements of R.25 to express trusts, but fully covers all other types of legal arrangements (depending on the relative material importance and risk of those other types). Conversely, an LC rating could be justified if trusts or

implemented in relation to beneficial ownership information, as opposed to criterion 25.8 which should focus on whether the information collected is adequate, accurate and up-to-date. This means that if assessors note that the relevant information is not adequate, accurate or up-to-date, such deficiencies should be noted under criterion 25.8 (not elsewhere in other criteria).

4 When assessing criteria 25.7(a) and (c) and 25.10, assessors should also refer to the third paragraph of the *Note to Assessors* for R.15.

Scope extends to express trusts and other similar arrangements

25.1 The requirements of Recommendation 25 apply to all *legal arrangements* meaning *express trusts* (as defined in the Glossary of the FATF Recommendations) and other similar arrangements. Examples of other similar arrangements (for AML/CFT purposes) may include but are not limited to fiducie, certain types of Treuhand, fideicomiso and Waqf.[131]

25.2 Countries with express trusts and other similar legal arrangements governed under their law[132] should have mechanisms that:

a) identify the different types, forms and basic features of express trusts and/or other similar legal arrangements;

b) identify and describe the processes for: (i) the setting up of those legal arrangements; and (ii) the obtaining of basic[133] and beneficial ownership information; and

c) make the above information referred to in (a) and (b) publicly available.

other types of legal arrangements (which are also materially important in the context of the assessed country) are subject to most of the R.25 requirements, but other types of legal arrangements (which are not materially important or high risk) are completely outside the scope of R.25.

131 Except in countries where Waqf are legal persons under Recommendation 24.

132 This criterion covers the express trusts and other similar legal arrangements set up (i.e., created) under the law of the assessed country, but does not cover those that are set up (i.e., created) under the law of a different country even if they are administered in the assessed country.

133 In relation to a legal arrangement, basic information means the identifier of the legal arrangement (e.g. the name, the unique identifier such as a tax identification number or equivalent, where this exists), the trust deed (or equivalent) and purposes, if any, the residence of the trustee/equivalent or of the place from where the legal arrangement is administered.

a) Risk assessment and risk mitigation

25.3 Countries should assess the money laundering and terrorist financing risks associated with the following different types of trusts and other similar legal arrangements and take appropriate steps to manage and mitigate the risks that they identify:[134]

a) governed under their law;

b) which are administered in their country or for which the trustee or equivalent resides in their country; and

c) types of foreign legal arrangements that have sufficient links[135] with their country;

b) Basic and Beneficial ownership information

25.4 Countries should require trustees of any express trust[136] and persons holding an equivalent position in a similar legal arrangement, that are residents in their country or that administer any express trusts or similar legal arrangements in their country:

a) to obtain and hold adequate, accurate, and up-to-date[137] beneficial ownership information[138] [139] regarding the trust and other similar legal arrangements. This should include information on the identity of: (i) the settlor(s), (ii) the trustee(s), (iii) the protectors (if any); (iv) each beneficiary(ies) or, where applicable, the class of beneficiaries[140] and objects of a power; and (v) any other natural person(s) exercising ultimate effective control over the trust. For a similar legal arrangement, this should include persons holding equivalent positions;

---

134 This could be done through national and/or supranational measures. These could include requiring beneficial ownership information on some types of foreign legal arrangements to be held as set out under paragraph 5 of the INR25.

135 Countries may determine what is considered a sufficient link on the basis of risk. Examples of sufficiency tests may include, but are not limited to, when the trust/similar legal arrangement or a trustee or a person holding an equivalent position in a similar legal arrangement has significant and ongoing business relations with financial institutions or DNFBPs, has significant real estate/other local investment, or is a tax resident, in the country.

136 References to a *trust* in the Methodology criteria for R.25 mean *express trusts,* as defined in the Glossary to the FATF Recommendations.

137 *Note to assessors:* If assessors note that the relevant information is not "adequate, accurate or up-to-date, such deficiencies should be noted under criterion 25.8 (not elsewhere in other criteria). See also paragraph 3 of the *Note to assessors* above.

138 Beneficial ownership information for legal arrangements is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(ii) and the Glossary.

139 *Note to assessors:* If assessors note that the relevant information is not "adequate, accurate or up-to-date", such deficiencies should be noted under criterion 25.8 (not elsewhere in other criteria). See also paragraph 3 of the *Note to Assessors* above.

140 Where there are no ascertainable beneficiaries at the time of setting up the trust, the trustee should obtain and hold information on the class of beneficiaries and its characteristics, and objects of a power. Following a risk-based approach, countries may decide that it is not necessary to identify the individual beneficiaries of certain charitable or statutory permitted non-charitable trusts.

b) where the parties to the trusts or other similar legal arrangements are legal persons or arrangements, to also obtain and hold adequate, accurate, and up-to-date basic[141] and beneficial ownership information of the legal persons or arrangements; and

c) to hold basic information on other regulated agents of, and service providers to, the trust and similar legal arrangements, including but not limited to investment advisors or managers, accountants, and tax advisors.

25.5 Trustees and persons holding equivalent positions in similar legal arrangements should be required to maintain the information referred to in criterion 25.4 for at least five years after their involvement with the trust or similar legal arrangement ceases.

25.6 Countries should require that any information held pursuant to criterion 25.4 above should be kept accurate and up-to-date, and the information should be updated within a reasonable period following any change.

25.7 Countries should take measures to ensure that trustees or persons holding equivalent positions in similar legal arrangements:

a) disclose their status to financial institutions and DNFBPs when, in their function, forming a business relationship or carrying out an occasional transaction above the threshold;

b) cooperate to the fullest extent possible with competent authorities, and are not prevented by law or enforceable means from providing those authorities with necessary information relating to the trust or other similar legal arrangements;[142] and

c) are not prevented by law or enforceable means from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership of the trust or similar legal arrangement and any assets of the trust or legal arrangement to be held or managed under the terms of the business relationship.

141 See footnote 135 above.

142 Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

c) Timely access to adequate, accurate and up-to-date information

25.8 Countries should have mechanisms that ensure that information on trusts and other similar legal arrangements, including information provided in accordance with criteria 25.7 and 25.9, is adequate,[143] accurate[144] and up-to-date.[145] [146]

25.9 In order to ensure that adequate, accurate and up-to-date information[147] on the basic and beneficial ownership of the trusts or other similar legal arrangements, trustees and trust assets, is accessible efficiently and in a timely manner by competent authorities, other than through trustees or persons holding an equivalent position in a similar legal arrangement, on the basis of risk, context and materiality, countries should consider using any of the following sources of information as necessary:

a) A public authority or body holding information on the beneficial ownership of trusts or other similar arrangements (e.g. in a central registry of trusts; or in asset registries for land, property, vehicles, shares or other assets that hold information on the beneficial ownership of trusts and other similar legal arrangements, which own such assets). Information need not be held by a single body only.[148]

b) Other competent authorities that hold or obtain information on trusts/similar legal arrangements and trustees/their equivalents (e.g. tax authorities, which collect information on assets and income relating to trusts and other similar legal arrangements).

c) Other agents or service providers, including trust and company service providers, investment advisors or managers, accountants, lawyers, or financial institutions.

---

143 *Adequate* information is information that is sufficient to identify the natural persons who are the beneficial owner(s), and their role in the legal arrangement. This means the settlor(s), trustee(s), protector(s) (if any), beneficiary(ies) or, where applicable, the class of beneficiaries, and objects of a power, and any other person exercising ultimate effective control over the trusts. For a similar legal arrangement, this should include persons holding equivalent positions. Where the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified.

144 *Accurate* information is information, which has been verified to confirm its accuracy by verifying the identity and status of the beneficial owner using reliable documents, data or information. The extent of verification measures may vary according to the specific level of risk.

145 *Up-to-date* information is information which is as current and up-to-date as possible, and is updated within a reasonable period following any change. For beneficiary(ies) of trusts/similar legal arrangement that are designated by characteristics or by class, trustees/equivalent are not expected to obtain fully adequate and accurate information until the person becomes entitled as beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights, as per the risk-based approach.

146 *Note to assessors:* If assessors note that the relevant information is not "adequate, accurate or up-to-date", such deficiencies should be noted under criterion 25.8 (not elsewhere in other criteria). See also paragraph 3 of the *Note to Assessors* above.

147 Ibid.

148 A body could record beneficial ownership information alongside other information (e.g. tax information), or the source of information could take the form of multiple registries (e.g. for provinces or districts, for sectors, or for specific types of legal arrangements), or of a private body entrusted with this task by the public authority.

25.10 Countries should ensure that competent authorities, and in particular law enforcement authorities and FIUs, should have all the powers necessary to obtain timely access to the information held by trustees, persons holding equivalent positions in similar legal arrangements, and other parties, in particular information held by financial institutions and DNFBPs on:

a) the basic and beneficial ownership of the legal arrangement;

b) the residence of the trustees and their equivalents; and

c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees or their equivalents with which they have a business relationship, or for which they undertake an occasional transaction.

d) Liability and sanctions

25.11 Countries should ensure that:

a) there are clear responsibilities to comply with the requirements of the Interpretive Note to Recommendation 25;

b) trustees or persons holding equivalent positions in similar legal arrangements are either:

i legally liable for any failure to perform the duties relevant to meeting the obligations in criterion 25.4 to 25.7;[149] or

ii that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply;[150] and

c) there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to grant to competent authorities timely access to information regarding the trust referred to in criteria 25.4 and 25.5.

e) International cooperation

25.12 Countries should rapidly, constructively and effectively provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements on the basis set out in Recommendations 37 and 40. This should include:

d) not placing unduly restrictive conditions on the exchange of information or assistance e.g., refuse a request on the grounds that it involves fiscal (including tax) matters, bank secrecy, etc.;

149 Countries need not include the requirements of criteria 25.4 to 25.7 and 25.11 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

150 This does not affect the requirements for effective, proportionate, and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

e) facilitating access by foreign competent authorities to any information held by registries or other domestic authorities;

f) exchanging domestically available information on the trusts or other legal arrangement;

g) using their competent authorities' powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts; and

h) to facilitate rapid, constructive and effective and effective international cooperation, where possible, designating and making publicly known the agency(ies) responsible for responding to all international requests for beneficial ownership information, consistent with countries' approach to access to beneficial ownership information. To this end, countries should consider keeping information held or obtained for the purpose of identifying beneficial ownership in a readily accessible manner.

RECOMMENDATION 26 REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *beneficial owner, competent authorities, Core Principles, country, currency, financial institutions, money or value transfer service, risk, shell bank, should, supervisors*, and *terrorist financing (TF)*.

26.1 Countries should designate one or more supervisors that have responsibility for regulating and supervising (or monitoring) financial institutions' compliance with the AML/CFT requirements.

Market Entry

26.2 Core Principles financial institutions should be required to be licensed. Other financial institutions, including those providing a money or value transfer service or a money or currency changing service, should be licensed or registered. Countries should not approve the establishment, or continued operation, of shell banks.

26.3 Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, in a financial institution.

Risk-based approach to supervision and monitoring

26.4 Financial institutions should be subject to:

(a) *for core principles institutions* - regulation and supervision in line with the core principles,[151] where relevant for AML/CFT, including the application of consolidated group supervision for AML/CFT purposes.

(b) *for all other financial institutions* - regulation and supervision or monitoring, having regard to the ML/TF risks in that sector. At a minimum, for *financial institutions providing a money or value transfer service, or a money or currency changing service* - systems for monitoring and ensuring compliance with national AML/CFT requirements.

[151] The Core Principles which are relevant to AML/CFT include: Basel Committee on Banking Supervision (BCBS) Principles 1-3, 5-9, 11-15, 26, and 29; International Association of Insurance Supervisors (IAIS) Principles 1, 3-10, 18, 21-23, and 25; and International Organization of Securities Commission (IOSCO) Principles 24, 28, 29 and 31; and Responsibilities A, B, C and D. Assessors may refer to existing assessments of the country's compliance with these Core Principles, where available.

26.5 The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions or groups should be determined on the basis of:

(a) the ML/TF risks and the policies, internal controls and procedures associated with the institution or group, as identified by the supervisor's assessment of the institution's or group's risk profile;

(b) the ML/TF risks present in the country; and

(c) the characteristics of the financial institutions or groups, in particular the diversity and number of financial institutions and the degree of discretion allowed to them under the risk-based approach.

26.6 The supervisor should review the assessment of the ML/TF risk profile of a financial institution or group (including the risks of non-compliance) periodically, and when there are major events or developments in the management and operations of the financial institution or group.

RECOMMENDATION 27 POWERS OF SUPERVISORS

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *financial institutions, should,* and *supervisors*.

28.1 Supervisors should have powers to supervise or monitor and ensure compliance by financial institutions with AML/CFT requirements.

28.2 Supervisors should have the authority to conduct inspections of financial institutions.

28.3 Supervisors should be authorised to compel[152] production of any information relevant to monitoring compliance with the AML/CFT requirements.

28.4 Supervisors should be authorised to impose sanctions in line with Recommendation 35 for failure to comply with the AML/CFT requirements. This should include powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's licence.

152 The supervisor's power to compel production of or to obtain access for supervisory purposes should not be predicated on the need to require a court order.

RECOMMENDATION 28 REGULATION AND SUPERVISION OF DNFBPS

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *beneficial owner, competent authorities, country, designated non-financial businesses and professions (DNFBP); risk, self-regulatory body (SRB), should*, and *terrorist financing (TF)*.

Casinos

28.1 Countries should ensure that casinos are subject to AML/CFT regulation and supervision. At a minimum:

a Countries should require casinos to be licensed.

b Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, or being an operator of a casino.

c Casinos should be supervised for compliance with AML/CFT requirements.

DNFBPs other than casinos

28.2 There should be a designated competent authority or SRB responsible for monitoring and ensuring compliance of DNFBPs with AML/CFT requirements.

28.3 Countries should ensure that the other categories of DNFBPs are subject to systems for monitoring compliance with AML/CFT requirements.

28.4 The designated competent authority or self-regulatory body (SRB) should:

(a) have adequate powers to perform its functions, including powers to monitor compliance;

(b) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function in a DNFBP; and

(c) have sanctions available in line with Recommendation 35 to deal with failure to comply with AML/CFT requirements.

All DNFBPs

28.5 Supervision of DNFBPs should be performed on a risk-sensitive basis, including:

(a) determining the frequency and intensity of AML/CFT supervision of DNFBPs on the basis of their understanding of the ML/TF risks, taking into consideration the characteristics of the DNFBPs, in particular their diversity and number; and

(b) taking into account the ML/TF risk profile of those DNFBPs, and the degree of discretion allowed to them under the risk-based approach, when assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs.

RECOMMENDATION 29 FINANCIAL INTELLIGENCE UNITS (FIU)

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, country, foreign counterparts*, and *should*.

29.1 Countries should establish an FIU with responsibility for acting as a national centre for receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing; and for the dissemination of the results of that analysis.[153]

29.2 The FIU should serve as the central agency for the receipt of disclosures filed by reporting entities, including:

(a) Suspicious transaction reports filed by reporting entities as required by Recommendation 20 and 23; and

(b) any other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

29.3 The FIU should:[154]

(a) in addition to the information that entities report to the FIU, be able to obtain and use additional information from reporting entities, as needed to perform its analysis properly; and

(b) have access to the widest possible range[155] of financial, administrative and law enforcement information that it requires to properly undertake its functions.

29.4 The FIU should conduct:

(a) operational analysis, which uses available and obtainable information to identify specific targets, to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences and terrorist financing; and

153 Considering that there are different FIU models, Recommendation 29 does not prejudge a country's choice for a particular model, and applies equally to all of them.

154 In the context of its analysis function, an FIU should be able to obtain from any reporting entity additional information relating to a suspicion of ML/TF. This does not include indiscriminate requests for information to reporting entities in the context of the FIU's analysis (e.g., "fishing expeditions").

155 This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate commercially held data.

(b) strategic analysis, which uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns.

29.5 The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities, and should use dedicated, secure and protected channels for the dissemination.

29.6 The FIU should protect information by:

(a) having rules in place governing the security and confidentiality of information, including procedures for handling, storage, dissemination, and protection of, and access to, information;

(b) ensuring that FIU staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information; and

(c) ensuring that there is limited access to its facilities and information, including information technology systems.

29.7 The FIU should be operationally independent and autonomous, by:

(a) having the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or forward or disseminate specific information;

(b) being able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information;

(c) when it is located within the existing structure of another authority, having distinct core functions from those of the other authority; and

(d) being able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

29.8 Where a country has created an FIU and is not an Egmont Group member, the FIU should apply for membership in the Egmont Group. The FIU should submit an unconditional application for membership to the Egmont Group and fully engage itself in the application process.

RECOMMENDATION 30 RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, confiscation, country, proceeds, property, should, terrorist financing (TF),* and *terrorist financing offence*.

30.1 There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, associated predicate offences and terrorist financing offences are properly investigated, within the framework of national AML/CFT policies.

30.2 Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related ML/TF offences during a parallel financial investigation,[156] or be able to refer the case to another agency to follow up with such investigations, regardless of where the predicate offence occurred.

30.3 There should be one or more designated competent authorities to expeditiously identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime.

30.4 Countries should ensure that Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, *per se*, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.

30.5 If anti-corruption enforcement authorities are designated to investigate ML/TF offences arising from, or related to, corruption offences under Recommendation 30, they should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.

156 A '*parallel financial investigation*' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s).

A '*financial investigation*' means an enquiry into the financial affairs related to a criminal activity, with a view to: (i) identifying the extent of criminal networks and/or the scale of criminality; (ii) identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and (iii) developing evidence which can be used in criminal proceedings.

RECOMMENDATION 31 POWERS OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *accounts, competent authorities, country, designated non-financial businesses and professions (DNFBP); financial institutions, legal persons, should*, and *terrorist financing (TF)*.

31.1 Competent authorities conducting investigations of money laundering, associated predicate offences and terrorist financing should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for:

(a) the production of records held by financial institutions, DNFBPs and other natural or legal persons;

(b) the search of persons and premises;

(c) taking witness statements; and

(d) seizing and obtaining evidence.

31.2 Competent authorities conducting investigations should be able to use a wide range of investigative techniques for the investigation of money laundering, associated predicate offences and terrorist financing, including:

(a) undercover operations;

(b) intercepting communications; (

(c) accessing computer systems; and

(d) controlled delivery.

31.3 Countries should have mechanisms in place:

(a) to identify, in a timely manner, whether natural or legal persons hold or control accounts; and

(b) to ensure that competent authorities have a process to identify assets without prior notification to the owner.

31.4 Competent authorities conducting investigations of money laundering, associated predicate offences and terrorist financing should be able to ask for all relevant information held by the FIU.

RECOMMENDATION 32 CASH COURIERS

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: bearer negotiable instruments, competent authorities, confiscation, country, currency, false declaration, false disclosure, physical cross-border transportation, related to terrorist financing or money laundering, should, and terrorist financing (TF).

Recommendation 32 may be implemented on a supra-national basis by a supra-national jurisdiction, such that only movements that cross the external borders of the supra-national jurisdiction are considered to be cross-border for the purposes of Recommendation 32. Such arrangements are assessed on a supra-national basis, on the basis set out in Paragraphs 28-32 of the Introduction.

32.1 Countries should implement a declaration system or a disclosure system for incoming and outgoing cross-border transportation of currency and bearer negotiable instruments (BNIs). Countries should ensure that a declaration or disclosure is required for all physical cross-border transportation, whether by travellers or through mail and cargo, but may use different systems for different modes of transportation.

32.2 In a declaration system, all persons making a physical cross-border transportation of currency or BNIs, which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15 000, should be required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system:

(a) A written declaration system for all travellers;

(b) A written declaration system for all travellers carrying amounts above a threshold; and/or

(c) An oral declaration system for all travellers.

32.3 In a disclosure system, travellers should be required to give a truthful answer and provide the authorities with appropriate information upon request, but are not required to make an upfront written or oral declaration.

32.4 Upon discovery of a false declaration or disclosure of currency or BNIs or a failure to declare or disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs, and their intended use.

32.5 Persons who make a false declaration or disclosure should be subject to proportionate and dissuasive sanctions, whether criminal, civil or administrative.

32.6 Information obtained through the declaration/disclosure process should be available to the FIU either through: (a) a system whereby the FIU is notified about suspicious cross-border transportation incidents; or (b) by making the declaration/disclosure information directly available to the FIU in some other way.

32.7 At the domestic level, countries should ensure that there is adequate co-ordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

32.8 Competent authorities should be able to stop or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/TF may be found in cases:

(a) where there is a suspicion of ML/TF or predicate offences; or

(b) where there is a false declaration or false disclosure.

32.9 Countries should ensure that the declaration/disclosure system allows for international co-operation and assistance, in accordance with Recommendations 36 to 40. To facilitate such co-operation, information[157] shall be retained when:

(a) a declaration or disclosure which exceeds the prescribed threshold is made; or

(b) there is a false declaration or false disclosure; or

(c) there is a suspicion of ML/TF.

32.10 Countries should ensure that strict safeguards exist to ensure proper use of information collected through the declaration/disclosure systems, without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

32.11 Persons who are carrying out a physical cross-border transportation of currency or BNIs that are related to ML/TF or predicate offences should be subject to: (a) proportionate and dissuasive sanctions, whether criminal, civil or administrative; and (b) measures consistent with Recommendation 4 which would enable the confiscation of such currency or BNIs.

157 At a minimum, the information should set out (i) the amount of currency or BNIs declared, disclosed or otherwise detected, and (ii) the identification data of the bearer(s).

RECOMMENDATION 33 STATISTICS

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *country, property, seize, should,* and *terrorist financing (TF).*

33.1 Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems.[158] This should include keeping statistics on:

(a) STRs, received and disseminated;

(b) ML/TF investigations, prosecutions and convictions;

(c) Property frozen; seized and confiscated; and

(d) Mutual legal assistance or other international requests for co-operation made and received.

158 For purposes of technical compliance, the assessment should be limited to the four areas listed below.

RECOMMENDATION 34 GUIDANCE AND FEEDBACK

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, designated non-financial businesses and professions (DNFBP); financial institutions, self-regulatory body (SRB), should,* and *supervisors*.

34.1 Competent authorities, supervisors, and SRBs should establish guidelines and provide feedback, which will assist financial institutions and DNFBPs in applying national AML/CFT measures, and in particular, in detecting and reporting suspicious transactions.

RECOMMENDATION 35 SANCTIONS

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *country, designated non-financial businesses and professions (DNFBP); financial institutions, legal persons,* and *should*.

35.1 Countries should ensure that there is 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.[159]

35.2 Sanctions should be applicable not only to financial institutions and DNFBPs but also to their directors and senior management.

[159] The sanctions should be directly or indirectly applicable for a failure to comply. They need not be in the same document that imposes or underpins the requirement, and can be in another document, provided there are clear links between the requirement and the available sanctions.

RECOMMENDATION 36 INTERNATIONAL INSTRUMENTS

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *country*, and *should*.

36.1 Countries should become a party to the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption (the Merida Convention) and the Terrorist Financing Convention.

36.2 Countries should fully implement[160] the Vienna Convention, the Palermo Convention, the Merida Convention[161] and the Terrorist Financing Convention.

160 The relevant articles are: the Vienna Convention (Articles 3-11, 15, 17 and 19), the Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31, & 34), the Merida Convention (Articles 14-17, 23-24, 26-31, 38, 40, 43-44, 46, 48, 50-55, 57-58), and the Terrorist Financing Convention (Articles 2-18).

161 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.

RECOMMENDATION 37 MUTUAL LEGAL ASSISTANCE

Note to Assessors*:*

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, country, designated non-financial businesses and professions (DNFBP); financial institutions, fundamental principles of domestic law, legal persons, should*, and *terrorist financing (TF)*.

37.1 Countries should have a legal basis that allows them to rapidly provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions and related proceedings.

37.2 Countries should use a central authority, or another established official mechanism, for the transmission and execution of requests. There should be clear processes for the timely prioritisation and execution of mutual legal assistance requests. To monitor progress on requests, a case management system should be maintained.

37.3 Mutual legal assistance should not be prohibited or made subject to unreasonable or unduly restrictive conditions.

37.4 Countries should not refuse a request for mutual legal assistance:

(a) on the sole ground that the offence is also considered to involve fiscal matters; or

(b) on the grounds of secrecy or confidentiality requirements on financial institutions or DNFBPs, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies.

37.5 Countries should maintain the confidentiality of mutual legal assistance requests that they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry.

37.6 Where mutual legal assistance requests do not involve coercive actions, countries should not make dual criminality a condition for rendering assistance.

37.7 Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

37.8 Powers and investigative techniques that are required under Recommendation 31 or otherwise available to domestic competent authorities should also be available for use in response to requests for mutual legal assistance, and, if consistent with the domestic

framework, in response to a direct request from foreign judicial or law enforcement authorities to domestic counterparts. These should include:

(a) all of the specific powers required under Recommendation31 relating to the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons, and the taking of witness statements; and

(b) a broad range of other powers and investigative techniques.

RECOMMENDATION 38 MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION

Note to Assessors:

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *confiscation, country, freeze, fundamental principles of domestic law, non-conviction based confiscation, proceeds, property, seize, should*, and *terrorist financing (TF)*.

38.1 Countries should have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize, or confiscate:

(a) laundered property from,

(b) proceeds from,

(c) instrumentalities used in, or

(d) instrumentalities intended for use in money laundering, predicate offences, or terrorist financing; or

(e) property of corresponding value.

38.2 Countries should have the authority to provide assistance to requests for co-operation made on the basis of non-conviction based confiscation proceedings and related provisional measures, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown, unless this is inconsistent with fundamental principles of domestic law.

38.3 Countries should have: (a) arrangements for co-ordinating seizure and confiscation actions with other countries; and (b) mechanisms for managing, and when necessary disposing of, property frozen, seized or confiscated.

38.4 Countries should be able to share confiscated property with other countries, in particular when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

RECOMMENDATION 39 EXTRADITION

Note to Assessors*:*

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *competent authorities, country, fundamental principles of domestic law, should,* and *terrorist financing (TF)*.

39.1 Countries should be able to execute extradition requests in relation to ML/TF without undue delay. In particular, countries should:

(a) ensure ML and TF are extraditable offences;

(b) ensure that they have a case management system, and clear processes for the timely execution of extradition requests including prioritisation where appropriate; and

(c) not place unreasonable or unduly restrictive conditions on the execution of requests.

39.2 Countries should either:

(a) extradite their own nationals; or

(b) where they do not do so solely on the grounds of nationality, should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request.

39.3 Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

39.4 Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms[162] in place.

[162] Such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

RECOMMENDATION 40 OTHER FORMS OF INTERNATIONAL CO-OPERATION

Note to Assessors*:*

Assessors should refer to the following Glossary definitions when assessing this Recommendation: *accounts, beneficial owner, competent authorities, Core Principles, country, designated non-financial businesses and professions (DNFBP); financial institutions, foreign counterparts, law, proceeds, should, supervisors*, and *terrorist financing (TF)*.

General Principles

40.1 Countries should ensure that their competent authorities can rapidly provide the widest range of international co-operation in relation to money laundering, associated predicate offences and terrorist financing. Such exchanges of information should be possible both spontaneously and upon request.

40.2 Competent authorities should:

(a) have a lawful basis for providing co-operation;

(b) be authorised to use the most efficient means to co-operate;

(c) have clear and secure gateways, mechanisms or channels that will facilitate and allow for the transmission and execution of requests;

(d) have clear processes for the prioritisation and timely execution of requests; and

(e) have clear processes for safeguarding the information received.

40.3 Where competent authorities need bilateral or multilateral agreements or arrangements to co-operate, these should be negotiated and signed in a timely way, and with the widest range of foreign counterparts.

40.4 Upon request, requesting competent authorities should provide feedback in a timely manner to competent authorities from which they have received assistance, on the use and usefulness of the information obtained.

40.5 Countries should not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of exchange of information or assistance. In particular, competent authorities should not refuse a request for assistance on the grounds that:

(a) the request is also considered to involve fiscal matters; and/or

(b) laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies); and/or

(c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or

(d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

40.6 Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only for the purpose for, and by the authorities, for which the information was sought or provided, unless prior authorisation has been given by the requested competent authority.

40.7 Competent authorities should maintain appropriate confidentiality for any request for co-operation and the information exchanged, consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Competent authorities should be able to refuse to provide information if the requesting competent authority cannot protect the information effectively.

40.8 Competent authorities should be able to conduct inquiries on behalf of foreign counterparts, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

Exchange of Information between FIUs

40.9 FIUs should have an adequate legal basis for providing co-operation on money laundering, associated predicate offences and terrorist financing.[163]

40.10 FIUs should provide feedback to their foreign counterparts, upon request and whenever possible, on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

40.11 FIUs should have the power to exchange:

(a) all information required to be accessible or obtainable directly or indirectly by the FIU, in particular under Recommendation 29; and

(b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.

Exchange of information between financial supervisors

40.12 Financial supervisors should have a legal basis for providing co-operation with their foreign counterparts (regardless of their respective nature or status), consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

[163] FIUs should be able to provide co-operation regardless of whether their counterpart FIU is administrative, law enforcement, judicial or other in nature.

40.13 Financial supervisors should be able to exchange with foreign counterparts' information domestically available to them, including information held by financial institutions, in a manner proportionate to their respective needs.

40.14 Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other supervisors that have a shared responsibility for financial institutions operating in the same group:

(a) regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors;

(b) prudential information, in particular for Core Principles supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness; and

(c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

40.15 Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

40.16 Financial supervisors should ensure that they have the prior authorisation of the requested financial supervisor for any dissemination of information exchanged, or use of that information for supervisory and non-supervisory purposes, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation.

Exchange of information between law enforcement authorities

40.17 Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.

40.18 Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement co-operation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority.

40.19 Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangements to enable such joint investigations.

Exchange of information between non-counterparts

40.20 Countries should permit their competent authorities to exchange information indirectly[164] with non-counterparts, applying the relevant principles above. Countries should ensure that the competent authority that requests information indirectly always makes it clear for what purpose and on whose behalf the request is made.

164 Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country.

EFFECTIVENESS ASSESSMENT

Immediate Outcome 1	Money laundering and terrorist financing risks are identified, assessed and understood, policies are co-operatively developed and, where appropriate, actions co-ordinated domestically to combat money laundering and the financing of terrorism.

Characteristics of an effective system

A country properly identifies, assesses and understands its money laundering and terrorist financing risks. This includes the involvement of competent authorities and other relevant authorities and using a wide range of reliable information sources. The country uses the assessment(s) of risks as a basis for developing and prioritising AML/CFT policies and to mitigate the identified risks.

A country also co-operates and co-ordinates domestically to develop AML/CFT policies, communicating and implementing those policies in a co-ordinated way across appropriate channels. This includes effective co-operation and where appropriate, co-ordination including and timely information sharing, between different competent authorities for operational purposes related to AML/CFT. Over time, this results in substantial mitigation of money laundering, and terrorist financing risks.

This outcome relates primarily to Recommendations 1, 2, 33 and 34, and elements of R.15.

Note to Assessors:

1 Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: *competent authorities, country, designated non-financial businesses and professions (DNFBP); financial institutions, law, risk, self-regulatory body (SRB), should,* and *terrorist financing (TF)*.

2 Assessors are not expected to re-assess the country's assessment(s) of risks. Assessors, based on their views of the reasonableness of the assessment(s) of risks, and taking into account the context of the country, as set out in paragraphs 5-13 of the Methodology, should focus on how well the competent authorities have identified, assessed and understood the ML/TF risks facing the country, and then using their understanding of the risks in practice to inform policy development and actions to mitigate the risks.

3 Assessors should take into consideration their findings for this Immediate Outcome (IO) in their assessment of the other IOs.

Core Issues to be considered in determining if the Outcome is being achieved

1.1 How well does the country identify, assess, and understand its ML/TF risks?

1.2 How well do national AML/CFT policies and activities address the identified ML/TF risks?

1.3 To what extent are the results of the assessment(s) of ML/TF risks properly used to justify exemptions and support the application of enhanced measures for higher risk scenarios, or simplified measures for lower risk scenarios?

1.4 To what extent are the objectives and activities of the competent authorities and SRBs consistent with the evolving national AML/CFT policies and with the ML/TF risks identified?

1.5 To what extent do the competent authorities and SRBs co-operate and co-ordinate the development and implementation of policies[165] to combat ML/TF?[166]

1.6 To what extent do the competent authorities co-operate and, where appropriate, co-ordinate for operational purposes related to AML/CFT.

a) Examples of Information that could support the conclusions on Core Issues

1 The country's assessment(s) of its ML/TF risks (e.g., *types of assessment(s) produced; types of assessment(s) published / communicated*).

2 AML/CFT policies and strategies (e.g., *AML/CFT policies, strategies and statements communicated/published; engagement and commitment at the senior officials and political level*).

3 Information on engagement of relevant authorities at policy and operational levels (*e.g. frequency and* relevancy *of engagement on policies and legislation; use of both formal and informal communication and co-operation channels frameworks and mechanisms; cases of successful inter-agency coordination).*

b) Examples of Specific Factors that could support the conclusions on Core Issues

4 What are the methods, tools, and information used to develop, review and evaluate the conclusions of the assessment(s) of risks? How comprehensive are the information and data used?

5 How useful are strategic financial intelligence, analysis, typologies, and guidance?

6 Which competent authorities and relevant stakeholders (including financial institutions and DNFBPs) are involved in the assessment(s) of risks? How do they provide inputs to the national level ML/TF assessment(s) of risks, and at what stage?

---

165 Having regard to AML/CFT requirements and Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation) as needed.

166 Considering that there are different forms of co-operation and co-ordination between relevant authorities, core issues 1.5 and 1.6 do not prejudge a country's choice for a particular form and applies equally to all of them.

7 Is the assessment(s) of risks kept up-to-date, reviewed regularly and responsive to significant events or developments (including new threats and trends)?

8 To what extent is the assessment(s) of risks reasonable and consistent with the ML/TF threats, vulnerabilities and specificities faced by the country, including key structural elements and contextual factors such as stable institutions, the rule of law, and the level of corruption? Where appropriate, does it take into account risks identified by other credible sources?

9 Do the policies of competent authorities respond to changing ML/TF risks?

10 What framework(s), or body do the authorities use to ensure proper and regular co-operation and co-ordination of the national framework and development and implementation of policies to combat ML/TF, at the policymaking level? Does the framework(s) or body include all relevant authorities?

11 What mechanism(s) do the authorities use to ensure proper and regular co-operation and, where appropriate, co-ordination at the operational level, to combat ML/TF? Are the roles of each relevant authority clear? How is interagency work facilitated (e.g. are there joint teams or shared data platforms)?

12 Is interagency information sharing undertaken in a timely manner on a bilateral or multiagency basis as appropriate? Are the information needs and information sources of each relevant authority clear? Are there measures to facilitate timely flow of information among relevant authorities (e.g. standard formats and secure channels to facilitate timely flow of information)?

13 Are there adequate resources and expertise involved in conducting the assessment(s) of ML/TF risks, and for domestic co-operation and co-ordination to combat ML/TF?

Immediate Outcome 2	International co-operation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.

Characteristics of an effective system

The country provides constructive and timely information or assistance when requested by other countries. Competent authorities assist with requests to:

- locate and extradite criminals; and
- identify, freeze, seize, confiscate and share assets and provide information (including evidence, financial intelligence, supervisory and beneficial ownership information) related to money laundering, terrorist financing or associated predicate offences.

Competent authorities also seek international co-operation to pursue criminals and their assets. Over time, this makes the country an unattractive location for criminals (including terrorists) to operate in, maintain their illegal proceeds in, or use as a safe haven.

This outcome relates primarily to Recommendations 36 - 40 and also elements of Recommendations 9, 15, 24, 25 and 32.

Note to Assessors:

1 Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: *beneficial owner, competent authorities, confiscation, country, designated categories of offences, foreign counterparts, freeze, law, legal persons, proceeds, risk, seize, should, supervisors, terrorist*, and *terrorist financing (TF)*.

2 Assessors should consider how their findings on the specific role of relevant competent authorities in seeking and delivering international co-operation under this IO impacts other IOs. This includes how the country seeks international co-operation with respect to domestic cases when appropriate. Similarly, assessors should consider how their findings under other IOs may affect their assessment of how effectively competent authorities are seeking and providing international co-operation (while avoiding duplication).

3 When drafting the section on international co-operation, assessors should include an introductory paragraph identifying and explaining the team's findings on the overall importance of international co-operation in light of the assessed country's risk and context. When assessing the core issues, assessors should consider whether international

co-operation efforts are aligned with risk[167] including by taking into account (a) the overall extent, timeliness and prioritisation of co-operation on AML/CFT activities, (b) the nature or type of co-operation, (c) the offences or matters to which assistance or requests relates, and (d) the countries to which or from which the requests were made or received.

4 Assessors should give appropriate weight both to the quality and impact[168] of international co-operation as well as the quantity of co-operation requests made in light of its risk profile. Processes and procedures for seeking or providing co-operation may be relevant to the extent that they affect effectiveness, but assessors should avoid focusing excessively on these factors or repeating information covered in the technical compliance Annex.

5 The core issues are divided into 'formal' types of international co-operation (mutual legal assistance and extradition; core issues 2.1 and 2.2) and other, more 'informal' co-operation (e.g., direct or indirect communication between counterpart authorities, assistance via regional or international mechanisms, etc.; core issues 2.3 and 2.4). Assessors should consider the links between these two types of co-operation in the assessed country and how informal co-operation is used to support formal co-operation. In practice, informal co-operation will often be an essential element that underpins successful formal co-operation.

Core Issues to be considered in determining if the Outcome is being achieved

2.1. To what extent has the country provided constructive and timely mutual legal assistance and extradition to respond to requests to provide evidence related to ML, associated predicate offences and TF; to locate and extradite criminals; and to identify, freeze, seize and confiscate criminal assets and share confiscated assets? What is the quality of such assistance provided?

2.2. To what extent has the country sought mutual legal assistance and extradition in an appropriate and timely manner that contributes to obtaining evidence related to ML, associated predicate offences and TF; to locating and extraditing criminals; and to identifying, freezing, seizing, and confiscating criminal assets?

2.3. To what extent do the different competent authorities use other forms of international co-operation to seek information or assistance from foreign authorities in an appropriate and timely manner for AML/CFT purposes, including asset recovery? This should include all relevant types of information (such as financial information; financial intelligence; and basic or beneficial ownership information), and covers information and assistance from relevant

167 Noting that countries have little control over the number or type of requests received.

168 Noting that countries have limited control over how assistance provided is used, the impact of co-operation provided should not be a determinative factor, but may help assessors build a picture of the quality and proactivity of a country's international co-operation. Assessors should draw upon all available information, including case studies, feedback provided by other countries, and on the available statistics.

competent authorities (such as supervisors; FIUs; law enforcement agencies; and customs and tax authorities).

2.4. To what extent do the different competent authorities use other forms of international co-operation to provide information or assistance to foreign authorities in a constructive and timely manner (including spontaneously) for AML/CFT purposes, including asset recovery? This should include all relevant types of information (such as financial information; financial intelligence; and basic or beneficial ownership information), and covers other information and assistance from relevant competent authorities (such as supervisors; FIUs; law enforcement agencies; and customs and tax authorities).

a) Examples of Information that could support the conclusions on Core Issues

1 Evidence of handling and making requests for international co-operation with respect to extradition, mutual legal assistance and other forms of international co-operation (*e.g., number of requests made, received, processed, granted, or refused relating to different competent authorities (e.g., central authority, FIU, supervisors, and law enforcement agencies) and types of request; timeliness of response, including prioritisation of requests; cases of spontaneous dissemination / exchange*).

2 Types and number of co-operation arrangements with other countries (including bilateral and multilateral MOUs, treaties, co-operation based on reciprocity, involvement in relevant international or regional fora or networks, or other co-operation mechanisms).

3 Examples of: (a) making requests for international co-operation, particularly relating to the assessed *jurisdiction's* areas of high ML/TF risks, and (b) providing quality international co-operation (e.g*., making use of financial intelligence / evidence provided to or by the country (as the case may be); investigations conducted on behalf or jointly with foreign counterparts; extradition of suspects/criminals for ML/TF*).

4 Information on investigations, prosecutions, confiscation and repatriation/sharing of assets (e.g., *number of ML/TF investigations/ prosecutions, number and value of assets frozen and confiscated (including non-conviction-based confiscation) arising from international co-operation; value of assets repatriated or shared*).

5 Types of assistance and information provided/sought (e.g., account information; basic and beneficial *ownership* information of legal persons and arrangements; asset identification and tracing; information relevant to fit and proper checks for supervision; real estate and vehicle records; tax information; etc.).

6 Examples (including through case studies or feedback from other countries) of the country's contribution to international co-operation efforts (e.g. prosecutions, convictions, asset recovery by foreign competent authorities; fugitives located and returned; etc.).

b) Examples of Specific Factors that could support the conclusions on Core Issues

7 What operational measures are in place to ensure that appropriate safeguards are applied, requests are handled in a confidential manner to protect the integrity of the process (*e.g.,* investigations and inquiry), and information exchanged is used for authorised purposes?

8 What mechanisms (including case management systems) are used among the different competent authorities to receive, assess, prioritise and respond to requests for assistance?

9 What are the reasons for refusal in cases where assistance is not or cannot be provided?

10 What mechanisms (including case management systems) are used among the different competent authorities to select, prioritise and make requests for assistance?

11 How do different competent authorities ensure that relevant and accurate information is provided to the requested country to allow it to understand and assess the requests?

12 To what extent is routine and constructive feedback provided?

13 How well has the country worked with the requesting or requested country to avoid or resolve conflicts of jurisdiction or problems caused by poor quality information in requests?

14 How do competent authorities ensure that details of the contact persons and requirements for international co-operation requests are clear and easily available to requesting countries?

15 To what extent does the country prosecute its own nationals without undue delay in situations when it is unable by law to extradite them?

16 What measures and arrangements are in place to manage and repatriate assets confiscated at the request of other countries?

17 Are there aspects of the legal, operational or judicial process (*e.g.,* excessively strict application of dual criminality requirements, reliance on unreasonable or unduly restrictive grounds for refusal, deficiencies in R.3 (including the scope of designated categories of offences), etc.) that impede or hinder international co-operation?

18 To what extent are competent authorities exchanging information, indirectly, with non-counterparts?

19 Are adequate resources available, in line with the country's risk, for: (a) receiving, managing, coordinating and responding to incoming requests for co-operation; and (b) making and coordinating requests for assistance in a timely manner?

Immediate Outcome 3	Supervisor[169] appropriately supervise, monitor and regulate financial institutions and VASPs for compliance with AML/CFT requirements, and financial institutions and VASPs adequately apply AML/CFT preventive measures, and report suspicious transactions. The actions taken by supervisors, financial institutions and VASPs are commensurate with the risks.

Characteristics of an effective system

Risk based supervision and monitoring identifies, assesses and mitigates the money laundering and terrorist financing risks in the financial and VASP sectors by:

- preventing criminals and their associates from holding, or being the beneficial owner of, a significant or controlling interest or a management function in financial institutions and VASPs; and
- guiding, monitoring and enforcing compliance by financial institutions and VASPs to ensure that they have effective AML/CFT policies in place. Where issues are identified, appropriate measures based on risk are taken to address them.

Over time, supervision and monitoring improve the level of AML/CFT compliance, and discourage attempts by criminals to abuse the financial and VASP sectors, particularly in financial institutions and VASPs most exposed to money laundering and terrorist financing risks.

Financial institutions and VASPs understand the nature and level of their money laundering and terrorist financing risks; develop and apply AML/CFT policies (including group-wide policies), internal controls, and programmes to adequately mitigate those risks; apply appropriate CDD measures to identify and verify the identity of their customers (including the beneficial owners) and conduct ongoing monitoring; adequately detect and report suspicious transactions; and comply with other AML/CFT requirements. This ultimately leads to a reduction in money laundering and terrorist financing activity within these entities.

This outcome relates primarily to Recommendations 9-21, 26, 27, 34 and 35, and also elements of Recommendations 1, 29 and 40.

169 "Supervisors" is defined in the FATF Glossary and covers the supervision of financial institutions. R.15 extends this to VASPs. VASPs should be supervised by a competent authority (not an SRB). As regards financial institutions and VASPs, the definition of supervisor refers to designated competent authorities or non-public bodies.

Note to Assessors:[170]

1 Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: *accounts, beneficial owner, competent authorities, correspondent banking, country, designated non-financial businesses and professions (DNFBP); financial group, financial institutions, money or value transfer service (MVTS), politically exposed persons (PEPs), risk, shell bank, should, supervisors, terrorist financing (TF), virtual asset*, and *virtual asset service providers (VASPs)*.

2 Assessors should take into account the country's background, context and materiality, as well as the ML/TF risks identified. In particular, assessors should reflect on the core issues in line with the size, complexity and risk profiles of the sectors under analysis, and whether the activities and measures being taken to mitigate those risks are aligned with the identified risks. In addressing identified deficiencies, additional focus should be given to how these are weighted and their systemic impact, in order to ensure consistency with the risk based approach.

3 As noted in the General Interpretation and Guidance, regardless of how countries may choose to classify VASPs, they should be subject to adequate regulation and risk-based supervision or monitoring by a competent authority, consistent with R.26 and R.27. Assessors should therefore always conduct the effectiveness assessment of VASPs under IO.3. Where a country decides to prohibit VASPs, the effectiveness assessment will focus primarily on the detection and enforcement of the prohibition (core issue 3.6), and how well the country understands the ML/TF risks related to VASPs (core issue 3.2). See the Introduction to the Methodology for further guidance on other aspects that should be taken into account when assessing IO.3, particularly with regard to risk and context.

4 Assessors should also consider the relevant findings (including at the group level) on the level of international co-operation which supervisors are participating in *when* assessing IO.3 and IO.4.

5 *Assessors* are not expected to conduct an in-depth review of the operations of financial institutions, DNFBPs, and VASPs, but should consider, on the basis of evidence and interviews with supervisors, FIUs and other competent authorities, as well as the private sector, whether financial institutions, DNFBPs and VASPs have adequately assessed and understood their exposure to money laundering and terrorist financing risks; whether their policies, procedures and internal controls adequately address and mitigate these risks; and whether regulatory requirements (including STR reporting) are properly implemented.

170 These Notes to Assessors should be read as applicable to when assessing IO.3 and IO.4.

6 *Evidence* can include responses to questionnaires[171] by assessed countries and financial institutions/DNFBP and VASP, as well as case studies, information detailed in Examples of Information and/or Examples of Factors that could support conclusions on core issues as well as other information thought useful by and provided by the Assessed Country. Assessors may request additional information to corroborate findings during the course of the assessment (*including* during the onsite visit), to further understand how supervision and monitoring have improved the level of AML/CFT compliance and discouraged attempts by criminals to abuse the Financial/DNFBP or VASP sectors.

7 Assessors should assess the regulation, supervision and monitoring by supervisors, and the implementation of preventive measures by the private sector in a coherent manner. The two aspects are positively correlated where effective supervision *and* monitoring over time would result in more effective implementation of preventive measures by the private sector. Poor implementation of preventive measures by the private sector can suggest ineffective supervision or monitoring, except where significant legal deficiencies may have undermined the effectiveness of preventive measures. The overall assessment of IO.3 and IO.4 should thus equally combine the assessment of those two elements.

Core Issues to be considered in determining if the Outcome is being achieved

3.1. How well does licensing, registration or other controls implemented by supervisors or other authorities prevent, criminals and their associates from holding, or being the beneficial owner of a significant or controlling interest or holding a management function in financial institutions and VASPs? How well are breaches of such licensing or registration requirements detected and addressed as appropriate?

3.2. How well do the supervisors identify, understand, and promote financial institutions and VASPs understanding of ML/TF risks and AML/CFT obligations? This includes identifying and maintaining an understanding of the ML/TF risks in the different sectors and types of institutions, and of individual institutions and VASPs over time.

3.3. How well do financial institutions and VASPs understand the level and the nature of their ML/TF risks? This includes demonstrating understanding of the evolution of ML/TF risks over time.

3.4. How well do financial institutions and VASPs understand and apply AML/CFT obligations and mitigating measures and appropriate to their business activities, including as regards:

i the CDD and record-keeping measures (including in relation to beneficial ownership information and ongoing monitoring)?

171. In November 2017, Plenary approved optional structured formats which could be useful in the assessment of IO.4 (FATF/PLEN/M(2017)5). These include a checklist of questions that could be sent to FI/DNFPB/VASP and/or be a useful to guide discussions. See Annex B of FATF/ECG(2017)18/REV2.

ii the enhanced or specific measures for: (a) PEPs, (b) correspondent banking, (c) new technologies, (d) wire and virtual asset transfer rules, and (e) high-risk countries identified by the FATF?

iii their AML/CFT reporting obligations? What are the practical measures to prevent tipping off?

iv internal controls and procedures and audit requirements (including at group level where applicable) to ensure compliance with AML/CFT requirements?

v To what extent are there legal or regulatory requirements (e.g., financial secrecy) impeding implementation of AML/CFT obligations and mitigating measures?

3.5. With a view to mitigating the risks, how well do supervisors monitor and/or supervise the extent to which financial institutions and VASPs are complying with their AML/CFT requirements?

3.6. To what extent has monitoring and/or supervision, including outreach, training and applying remedial actions and/or effective, proportionate and dissuasive sanctions, where appropriate, had a demonstrable positive impact on compliance by financial institutions and VASPs over time?

a) Examples of Information that could support the conclusions on Core Issues

1 Contextual factors regarding the size, composition, and structure of the financial and VASP sectors and informal or unregulated sector (e.g., *number and types of financial institutions (including MVTS) and VASPs licensed or registered in each category (high, medium low risk, other); types of financial and VASP (including cross-border) activities; relative size, importance and materiality of sectors*).

2 Financial institutions and VASPs' information relating to risks and general levels of compliance (e.g., internal *risk* assessments, AML/CFT policies, procedures and programmes, trends and typologies reports).

3 Number and nature of license/registration applications approved/rejected, withdrawal of applications, and reasons for rejections/withdrawals (including information on fit and proper controls), as well as other related examples of illicit activity detected.

4 Supervisors' risk assessment and/or models, manuals and guidance on AML/CFT (e.g., *operations manuals for supervisory staff; publications outlining AML/CFT supervisory / monitoring approach; supervisory circulars, good and poor assessment practises, thematic studies; annual reports*).

5 Information on supervision (e.g., *on how the frequency, scope and nature of monitoring and inspections has been adjusted in line with risk, on-site and off-site or other type of visits, and the description of these main supervisory tools); nature and quality of supervisory communication with regulated entities (i.e., its comprehensiveness in relation to the subject-matter, identified risks and supervisory priorities)*.

6 Information on what additional measures or additional supervisory actions have been applied by the *competent* authorities in the home country to financial groups operating in host countries where the minimum AML/CFT requirements are less strict than the home country (*e.g. placing*

additional controls on the financial group, requesting the financial group to close down its operations in the host country).

7 *Information on supervisory findings and subsequent actions including number and nature of breaches identified; required remedial actions, sanctions and their enforcement* (e.g., including but not limited to number of warnings, *corrective actions, reprimands, directions, restrictions, fines) applied, examples of cases where sanctions and other remedial actions have been applied and improved AML/CFT compliance*). Information on how financial institutions and VASPs adjusted/improved their compliance practices in response to supervisor's actions

8 Where appropriate and applicable, and further to a risk-based approach to the adoption of technologies, information on how technology (e.g. advanced data analytics) is used by supervisors and the private sector, to support the understanding of obligations and/or risks identified, as well as assisting in AML/CFT tasks.

9 Information on supervisory engagement and outcomes of such engagement, with the industry, the FIU and other competent authorities, as well as other authorities in the country (e.g. prudential supervisor) on AML/CFT issues (e.g*., providing guidance and training, organising meetings or promoting interactions with financial institutions and VASPs*). This may include case studies of engagement with the private sector.

10 Examples of compliance by financial institutions and VASPs (e.g., sanitised cases; typologies on the misuse of financial institutions and VASPs). This could include, among other things, case studies of compliance best practices, compliance breaches (real/potential), examples of serious misconduct or harm, and information on how supervisory action made a direct/indirect impact on a firms' compliance controls.

11 Information on compliance by financial institutions and VASPs (e.g. frequency of internal AML/CFT compliance review commensurate with risks; frequency and quality of AML/CFT training; time taken to provide competent authorities with accurate and complete CDD information for AML/CFT purposes (upon request); accounts/relationships rejected due to incomplete CDD information; wire and VA transfers rejected due to insufficient requisite information; trends identified from transaction monitoring and reporting).

12 Information on STR reporting and other information as required by national legislation (e.g., number and quality of STRs submitted, and the value of associated transactions; number and proportion of STRs from different sectors; examples of STRs that contributed to investigations, quality of the information provided in the STR; the types, nature and trends in STR filings corresponding to ML/TF risks; average time taken from detection to filing an STR).

b) Examples of Specific Factors that could support the conclusions on Core Issues

13 What are the measures implemented to prevent the establishment or continued operation of shell banks in the country?

14 To what extent are "fit and proper" tests or other similar measures used with regard to persons holding senior management functions, holding a significant or controlling interest, or professionally accredited in financial institutions and VASPs?

15 What measures are taken to identify, license or register, monitor and sanction as appropriate, persons who carry out MVTS and virtual asset services or activities (including illegally)?

16 What measures do supervisors employ in order to assess the ML/TF risks of the sectors and entities they supervise/monitor? How often are the risk profiles reviewed, and what are the trigger events (e.g., changes in management or business activities)? How does the supervisor monitor the evolving risk environment and is it able to respond promptly?

17 To what extent are supervisors directing their focus effectively to higher or emerging ML/TF risks? Are there are appropriate, risk-based measures in place to address medium and lower risks effectively?

18 What measures and supervisory tools are employed to ensure that financial institutions and VASPs (including financial groups) are regulated and comply with their AML/CFT obligations? To what extent has this promoted the use of the formal financial system? Conversely, what measures are being taken in regard to the displacement of risk and to ensure that firms do not engage in blanket de-risking of sectors?

19 To what extent do the frequency, intensity and scope of on-site and off-site inspections relate to the risk profile of the financial institutions (including financial group) and VASPs?

20 Do supervisors have adequate resources and training to conduct supervision or monitoring for AML/CFT purposes, taking into account the size, complexity and risk profiles of the sector supervised or monitored?

21 What is the level of co-operation between supervisors and competent and other authorities in relation to AML/CFT (including financial group ML/TF risk management) issues? Under which circumstances supervisors share or seek information from other competent authorities with regard to AML/CFT issues (including market entry)?

22 What are the measures implemented to ensure that financial supervisors have operational independence so that they are not subject to undue influence on AML/CFT matters?

23 What are the measures in place to identify and deal with higher (and where relevant, lower) risk customers, business relationships, transactions, products and countries?

24 What are the policies, controls and procedures employed by financial institutions and VASPs to comply with AML/CFT obligations and how are these adjusted and adapted to the identified risks?

25 How well are financial institutions and VASPs conducting and documenting their ML/TF risk assessments, and keeping them up to date?

26 Does the manner in which AML/CFT measures are applied, by financial institutions and VASPs impede the legitimate use of the formal financial system, and hinder financial inclusion?

27 To what extent do the CDD and enhanced or specific measures vary according to ML/TF risks across different sectors / types of institution, and individual institutions? To what extent is business refused when CDD is incomplete? What is the relative level of compliance between international financial groups and domestic institutions?

28 To what extent is there reliance on third parties for compliance with AML/CFT requirements and how well are the controls applied?

29 How well do financial institutions and groups and VASPs and groups (as applicable) ensure adequate access to information by their AML/CFT compliance function?

30 Do internal policies and controls of the financial institutions and VASPs (including when operating in a group context where appropriate) enable timely review of: (i) complex or unusual transactions, (ii) potential STRs for reporting to the FIU, and (iii) potential false-positives? To what extent do the STRs reported contain complete, accurate and adequate information relating to the suspicious transaction?

31 How are AML/CFT policies and controls communicated to senior management and staff? What remedial actions and sanctions are taken by financial institutions and VASPs when AML/CFT obligations are breached?

32 Do financial institutions and VASPs have adequate resources and training to implement AML/CFT policies and controls relative to their size, complexity, business activities and risk profile?

33 How well is feedback provided, by competent authorities, to assist financial institutions and VASPs in detecting and reporting suspicious transactions?

Immediate Outcome 4	*Supervisors*[172] *appropriately supervise, monitor and regulate DNFBPs for compliance with AML/CFT requirements, and* DNFBPs adequately apply AML/CFT preventive measures commensurate with the risks, and report suspicious transactions.

Characteristics of an effective system

Risk based supervision and monitoring identifies, assesses and mitigates the money laundering and terrorist financing risks in DNFBPs by:

- preventing criminals and their associates from holding, or being the beneficial owner of, a significant or controlling interest or a management function in DNFBPs; and
- guiding, monitoring and enforcing compliance by DNFBPs to ensure that they have effective AML/CFT policies in place. Where issues are identified, appropriate measures based on risk are taken to address them.

Over time, supervision and monitoring improve the level of AML/CFT compliance, and discourage attempts by criminals to abuse the DNFBP sector, particularly in DNFBPs most exposed to money laundering and terrorist financing risks.

DNFBPs understand the nature and level of their money laundering and terrorist financing risks; develop and apply AML/CFT policies (including group-wide policies as appropriate), internal controls, and programmes to adequately mitigate those risks; apply appropriate CDD measures to identify and verify the identity of their customers (including the beneficial owners) and conduct ongoing monitoring; adequately detect and report suspicious transactions; and comply with other AML/CFT requirements. This ultimately leads to a reduction in money laundering and terrorist financing activity within these entities.

This outcome relates primarily to Recommendations 22, 23, 28, 34 and 35 and elements of Recommendations 1, 29 and 40.

Note to Assessors:

1 Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: accounts*, beneficial owner, competent authorities, country, designated non-financial*

172. For the purposes of supervision, monitoring and regulation of DNFBPs under IO.4, the reference to "supervisors" should be interpreted in accordance with the FATF Glossary.

businesses and professions (DNFBP); politically exposed persons (PEPs), risk, should, supervisors, and *terrorist financing (TF)*.

2 See notes to *assessors* (3-6) in IO3

Core Issues to be considered in determining if the Outcome is being achieved

4.1. How well do licensing, registration or other controls implemented by supervisors or other authorities prevent criminals and their associates from holding, or being the beneficial owner of a significant or controlling interest or holding a management function in DNFBPs? How well are breaches of such licensing or registration requirements detected and addressed as appropriate?

4.2. How well do supervisors identify, understand and promote regulated entities understanding of ML/TF risks and AML/CFT requirements? This includes identifying and maintaining an understanding of the ML/TF risks in different sectors and types of DNFBPs, and of individual DNFBPs over time.

4.3. How well do DNFBPs understand the nature of the level of their ML/TF risks? This includes demonstrating understanding of the evolution of ML/TF risks over time.

4.4. How well do DNFBPs understand and apply AML/CFT obligations and mitigating measures appropriate to their business activities, including as regards:

i. the CDD and record-keeping measures (including in relation to beneficial ownership information and ongoing monitoring)?

ii. the enhanced or specific measures for: (a) PEPs, (b) new technologies, (c) high-risk countries identified by the FATF?

iii. their AML/CFT reporting obligations? What are the practical measures to prevent tipping off?

iv. internal controls and procedures and audit requirements (including at group level where applicable) to ensure compliance with AML/CFT requirements?

v. To what extent are there legal or regulatory requirements impeding implementation of AML/CFT obligations and mitigating measures?

4.5 With a view to mitigating the risks, how well do supervisors, monitor and/or supervise the extent to which DNFBPs (including at group level where applicable), are complying with their AML/CFT requirements?

4.6 To what extent has monitoring and/or supervision, including, providing outreach, training and applying remedial actions and/or effective, proportionate and dissuasive sanctions where appropriate, had a demonstrable positive impact on compliance by DNFBPs over time?

a) Examples of Information that could support the conclusions on Core Issues

1 Contextual factors regarding the size, composition, and structure of the DNFBP sector and informal or unregulated sector (e.g., *number and types of DNFBPs licensed or registered in each category (high, medium, low risk, other; types of DNFBP (including cross-border) activities; relative size, importance and materiality of sectors*).

2 DNFBP's information relating to risks and general levels of compliance (e.g., *internal risk assessments, AML/CFT policies, procedures and programmes, trends and typologies reports*).

3 Number and nature of license/registration applications approved/rejected, withdrawal of applications, and reasons for rejections/withdrawals (including information from background checks or fit and proper controls), as well as other related examples of illicit activity detected, when applicable.

4 Supervisors' risk assessment and/or models, manuals and guidance on AML/CFT (*e.g., operations manuals for supervisory staff; publications outlining AML/CFT supervisory / monitoring approach; supervisory circulars, good and poor assessment practises, thematic studies; annual reports*).

5 Information on supervision (*e.g., on how the frequency, scope and nature of monitoring and inspections has been adjusted to consider risk, on-site and off-site; or other type of visits and the description of these main supervisory tools*); nature and quality of supervisory communication with regulated entities (i.e. its comprehensiveness in relation to the subject-matter, identified risks and supervisory priorities).

6 Information on supervisory findings and subsequent actions including number and nature of breaches identified; required remedial actions, sanctions and their enforcement (*e.g., including but not limited to number of warnings, corrective actions, reprimands, directions, restrictions, fines applied, examples of cases where sanctions and other remedial actions have been applied and improved AML/CFT compliance*). Information on how DNFBPs adjusted/improved their compliance practices in response to supervisor's actions.

7 Information on what additional measures or additional supervisory actions have been applied by the competent authorities in the home country to financial groups operating in host countries where the minimum AML/CFT requirements are less strict than the home country (*e.g. placing additional controls on the financial group, requesting the financial group to close down its operations in the host country*).

8 Where appropriate and applicable, and further to a risk based approach to the adoption of technologies, information on how technology (e.g. advanced data analytics) is used by supervisors and the private sector, to support the understanding of obligations and/or risks, as well as assisting in AML/CFT tasks.

9 Information on supervisory engagement and outcomes of such engagement, with the industry, the FIU and other competent authorities, as well as other authorities in the country (e.g. licensing or registration authority if different from supervisor) on AML/CFT issues (e.g., providing guidance and training, organising meetings or promoting interactions with DNFBPs). This may include case studies of engagement with the private sector.

10 Examples of compliance (e.g., *sanitised cases; typologies on the misuse of DNFBPs*). This could include case studies of compliance best practices, compliance breaches (real/potential), examples of serious misconduct or harm. Information on how supervisory action made a direct/indirect impact on a firms' compliance controls, among other.

11 Information on compliance by DNFBPs (e.g., *frequency of internal AML/CFT compliance review, commensurate with risks frequency and quality of AML/CFT training; time taken to provide competent authorities with accurate and complete CDD information for AML/CFT purposes; accounts/relationships rejected due to incomplete CDD information; wire transfers rejected due to insufficient requisite information; trends identified from transaction monitoring and reporting*).

12 Information on STR reporting and other information as required by national legislation (e.g., *number and quality of STRs submitted, and the value of associated transactions; number and proportion of STRs from different sectors; the types, nature and trends in STR filings corresponding to ML/TF risks; examples of STRs that contributed to investigations, quality of information provided in STRs, average time taken from detection to filing an STR*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

13 To what extent are "fit and proper" tests or other similar measures used with regard to persons holding senior management functions, holding a significant or controlling interest, or professionally accredited in DNFBPs?

14 What measures do supervisors employ in order to assess the ML/TF risks of the sectors and entities they supervise/monitor? How often are the risk profiles reviewed, and what are the trigger events (e.g., changes in management or business activities)? How does the supervisor monitor the evolving risk environment and is it able to respond promptly?

15 What measures and supervisory tools are employed to ensure that DFNBPs (including groups as appropriate) are regulated and comply with their AML/CFT obligations?

16 To what extent do the frequency, intensity and scope of supervisory tools/interventions including on-site and off-site inspections relate to the risk profile of the DNFBPs (including groups as appropriate)?

17 To what extent are supervisors directing their focus effectively to higher or emerging ML/TF risks? Are there are appropriate, risk-based strategies in place to address medium and lower risks effectively?

18 Do supervisors have adequate resources to conduct supervision or monitoring for AML/CFT purposes, taking into account the size, complexity and risk profiles of the sector supervised or monitored?

19 What is the level of co-operation between supervisors and competent and other authorities in relation to AML/CFT (including group ML/TF risk management as appropriate) issues? Under which circumstances do supervisors share or seek information from other competent authorities within and outside of the country where relevant with regard to AML/CFT issues (including market entry)?

20 What are the measures implemented to ensure that DNFBP supervisors have operational independence so that they are not subject to undue influence on AML/CFT matters?

21 What are the measures in place to identify and deal with higher (and where relevant, lower) risk customers, business relationships, transactions, products and countries?

22 To what extent do the CDD and enhanced or specific measures vary according to ML/TF risks across different sectors / types of institution, and individual institutions? To what extent is business refused when CDD is incomplete? What is the relative level of compliance between international DNFBP groups and where appropriate, internally?

23 To what extent is there reliance on third parties for compliance with AML/CFT requirements and how well are the controls applied?

24 How well do DNFBPs and groups (as applicable), ensure adequate access to information by the AML/CFT compliance function?

25 Do internal policies and controls of DNFBPs and, where appropriate, groups enable timely review of: (i) complex or unusual transactions, (ii) potential STRs for reporting to the FIU, and (iii) potential false-positives? To what extent do the STRs reported contain complete, accurate and adequate information relating to the suspicious transaction?

26 What are the policies, controls and procedures employed to comply with AML/CFT obligations and how are these adjusted and adapted to the identified risks?

27 How are AML/CFT policies and controls communicated to senior management and staff? What remedial actions and sanctions are taken by DNFBPs when AML/CFT obligations are breached?

28 How well are DNFBPs conducting and documenting their ML/TF risk assessments, and keeping them up to date?

29 Do DNFBPs have adequate resources to implement AML/CFT policies and controls relative to their size, complexity, business activities and risk profile?

30 How well is feedback provided, by competent authorities, to assist DNFBPs in detecting and reporting suspicious transactions?

Immediate Outcome 5	Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments.

Characteristics of an effective system:

A country properly identifies, assesses and understands its money laundering and terrorist financing risks associated with legal persons and arrangements created in the country, and foreign legal persons and arrangements that has sufficient links with the country. Measures are in place to:

- prevent legal persons and arrangements from being used for criminal purposes;
- make legal persons and arrangements sufficiently transparent; and
- ensure that adequate, accurate and up-to-date basic and beneficial ownership information is available on a timely basis.

Basic information is available publicly, and beneficial ownership information is available to competent authorities. Persons who breach these measures are subject to effective, proportionate and dissuasive sanctions. This results in legal persons and arrangements being unattractive for criminals to misuse for money laundering and terrorist financing.

This outcome relates primarily to Recommendations 24 and 25, and also elements of Recommendations 1, 10, 22, 37 and 40.

Note to Assessors:

1 Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: *bearer shares and bearer share warrants, beneficial owner, competent authorities, country, designated non-financial businesses and professions (DNFBP); financial institutions, legal arrangements, legal persons, nominee shareholder or director, risk, settlor, should, terrorist financing (TF),* and *trustee*.

2 Assessors should also consider the relevant findings in relation to the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent to which competent authorities seek and are able to provide the appropriate assistance in relation to identifying and exchanging information (including beneficial ownership information) for legal persons and arrangements, and providing input on these issues to the assessment of Immediate Outcome 2 (particularly Core Issues 2.3 and 2.4).

3 When assessing the core issues below, assessors should consider: the ML/TF risks associated with legal persons and arrangements created in the country, and foreign-created legal persons and arrangements that have sufficient links with the country; and whether the activities and measures it is taking to mitigate those risks are aligned with the identified risk.

4 The scope of core issue 5.1 is much narrower scope than core issue 1.1, which focuses on all ML/TF risks facing the country. Whether and to what extent deficiencies in core issue 5.1 may (or may not) impact the assessment of core issue 1.1 and rating for IO.1 will depend on the country's overall risks, materiality and context. See paragraphs 65 and 66 of the Methodology for further guidance.

5 When considering the *Examples of Information* and *Examples of Specific Factors that could* support *conclusion on core issues* in paragraphs 5, 6, 6bis, 8 and 14 below, assessors should also refer to the third paragraph of the Note to Assessors for R.15.

Core Issues to be considered in determining if the Outcome is being achieved

5.1 How well does the country identify, assess and understand its ML/TF risks associated with legal persons created in the country and foreign-created legal persons that have sufficient links with the country? How well does the country identify, assess and understand its ML/TF risks associated with legal arrangements governed under their law, administered in their country or for which the trustee or equivalent resides in their country, and types of foreign legal arrangements that have sufficient links with their country?

5.2 How well has the country implemented measures to prevent, manage and mitigate the risks associated with the misuse of legal persons and arrangements for ML/TF purposes, including measures to address the risk of misuse of bearer shares, bearer share warrants, nominee directors and nominee shareholders?

5.3 To what extent can relevant competent authorities obtain adequate, accurate and up-to-date basic and beneficial ownership information on all types of legal persons created in the country and foreign-created legal persons that present ML/TF risks and have sufficient links with their country, in a timely manner?

5.4 To what extent can relevant competent authorities obtain in a timely manner adequate, accurate and up-to-date information on: (a) the basic and beneficial ownership of the legal arrangement; (b) the residence of the trustees and their equivalents; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees or their equivalents with which they have a business relationship, or for which they undertake an occasional transaction? To what extent can relevant competent authorities obtain basic information on other regulated agents of, and service providers to, such trusts and similar legal arrangements, including but not limited to investment advisors or managers, accountants and tax advisors?

5.5 To what extent are effective, proportionate and dissuasive sanctions applied against persons who do not comply with the information requirements?

a) Examples of Information that could support conclusion on Core Issues

1 *Contextual* information on the types, forms and basic features of legal persons and arrangements in the jurisdiction, and any trends related to their creation (e.g., frequency of creation, prevalence, or changes in type or complexity).

2 *Information* on the role played by "gatekeepers" (e.g., *company service providers, accountants, legal professionals*) in the formation and administration of legal persons and arrangements.

3 *Information* on the role played by trustees or persons holding equivalent positions residing in the jurisdiction, the role of persons administering express trusts or similar legal arrangements in the jurisdiction, and disclosures made by trustees and persons holding equivalent positions (*e.g., any risk or threat assessments addressing the role of persons resident in the jurisdiction who are holding positions as trustees or equivalent positions, or administering express trusts or similar legal arrangements in the jurisdiction; industry studies or guidance on these issues*).

4 ML/TF risk assessments, typologies and examples of the misuse of domestic and foreign legal persons and arrangements (e.g., *frequency with which investigations find evidence of domestic or foreign legal persons and arrangements being used for ML/TF; frequency with which criminal investigations find evidence of bearer shares, bearer share warrants, nominee directors, nominee shareholders, company service providers, trustees or persons holding equivalent positions being used for ML/TF; legal persons misused for illegal activities being dismantled or struck-off*).

5 *Sources* of basic and beneficial ownership information (e.g., *types of public information available to financial institutions and DNFBPs; types of information held in the company registry or by the company, by a public authority or body or by an alternative mechanism*).

6 *Information* on how well registries and other sources of information are maintaining basic and BO information that is adequate, accurate and up to date (*e.g. how often basic and BO information on legal arrangements is reflected in registries; results of checks by registries at the time of registration and subsequently; supervisory findings of how well financial institutions/DNFBP are fulfilling their CDD/BO obligations; how often relevant entities (i.e., registries, reporting entities and companies) are verifying beneficial ownership information; to what extent relevant entities follow applicable policies to ensure that such identification is accurate and kept up-to-date; how frequently and to what extent the authorities conduct checks or supervision to confirm whether BO information is accurate and up-to-date; examples of cases where sanctions and/or other remedial actions have been applied and improved compliance in this area, whether complementary measures such as discrepancy reporting have been implemented to support the accuracy of BO information*).

7 *Additional* supplementary measures necessary to ensure the beneficial ownership of a company can be determined (*e.g., information held by regulators or stock exchanges, or obtained by financial institutions and/or DNFBPs in accordance with Recommendations 10 and 22; and considering in particular the extent to which the authorities are able to determine in a timely manner whether a company has or controls and account with a financial institution within the country*)?

8 *Information* on the extent to which bearer shares, bearer share warrants, nominee shareholders and nominee directors impede timely access to BO information (*e.g. information on their existence and prevalence; information on disclosures of nominee shareholder/director status or*

their licensing; information on the enforcement of prohibitions or actions to convert or immobilise existing bearer shares and bearer share warrants; examples of criminal investigations or prosecutions involving these obstacles to transparency).

9 Experiences of law enforcement and other relevant competent authorities (e.g., *where and how basic and beneficial ownership information for legal persons and arrangements is obtained in a timely manner; whether this information could be obtained from only the trustee or other sources, such as FIs and DNFBPs. information used in supporting investigation; the number, type and level of sanctions and other remedial actions imposed for failing to comply with the requirements of R.24 and R.25, and the impact of these on compliance*).

10 Other *information* (e.g., *information on existence of legal arrangements both foreign and domestic; responses (positive and negative) to incoming and outgoing requests for basic or beneficial ownership information received from other countries; time taken to respond and sources from which such BO information was obtained, information on the monitoring of quality of assistance*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

11 To what extent have the relevant authorities studied and assessed the risks of all relevant legal persons and arrangements both domestic and foreign with sufficient link to the country (e.g., as a standalone assessment or part of the broader assessment of the ML/TF risks in the country)? Based on the country's understanding of risks, how has the country implemented measures to address ML/TF risks posed by legal persons and arrangements?

12 What are the measures taken to manage and mitigate the risks identified in the risk assessment of legal persons (including prohibiting the issuance of new bearer shares and share warrants or taking risk-based measures for existing bearer shares and bearer share warrants, and taking risk-based measures on nominee shareholders and directors) and arrangements (including implementing the disclosure obligation for trustees and persons holding equivalent positions)?

13 How do relevant authorities ensure that accurate, adequate, and up-to-date basic and beneficial ownership information on legal persons and arrangements is maintained? Is the presence, adequacy and accuracy of such information of legal persons monitored, tested/certified or verified through a multi-pronged approach? Or through the use of different sources of information (such as a public authority or body holding BO information or tax information and gatekeepers and FIs) for legal arrangements? To what extent is information held or obtained for the purpose of identifying BO kept in a readily accessible manner?

14 To what extent is the time taken for legal persons to register changes to the required basic and beneficial ownership information to ensure that the information is adequate, accurate and up to date? Where applicable, to what extent are similar changes in legal arrangements registered in a timely manner?

15 To what extent can financial institutions and DNFBPs obtain adequate, accurate and up-to-date basic and beneficial ownership information on legal persons and arrangements? To what extent does the country facilitate access by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22 to: beneficial ownership and control information; and information that is held on trusts or other similar arrangements by the other

authorities, persons and entities referred to in criterion 25.9? What is the extent of information that trustees disclose to financial institutions and DNFBPs?

16 Do the relevant authorities have adequate resources to implement the measures adequately?

Immediate Outcome 6	Financial intelligence[173] and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.

Characteristics of an effective system

The FIU and other competent authorities access in a timely manner, a broad range of reports, data and other information that is relevant, accurate, and up-to-date, and which, assists them to perform their functions. The FIU has the resources and skills to conduct analysis and produces financial intelligence that supports the operational needs of other competent authorities. These other competent authorities have the resources and skills to perform their functions and where relevant, they also produce financial intelligence using available FIU data and other relevant information.

The FIU and other competent authorities co-operate and exchange information in a secure and regular manner, and a wide variety of financial intelligence and other relevant information is used to develop evidence, identify and trace assets, criminal proceeds or instrumentalities and investigate money laundering, associated predicate offences and terrorist financing.

This outcome relates primarily to Recommendations 29 to 32 and also elements of Recommendations 1, 2, 4, 8, 9, 15, 34 and 40.

Note to Assessors:

1 Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: *bearer negotiable instruments, competent authorities, country, currency, designated non-financial businesses and professions (DNFBP); financial institutions, foreign counterparts, proceeds, risk, should,* and *terrorist financing (TF)*.

2 This outcome includes the work that the FIU does to develop financial intelligence from its analysis of STRs and other data; and where relevant, the analysis other competent authorities do of reports and other data to develop financial intelligence, as well as their use of FIU products and other types of financial intelligence and other information.

3 Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent which FIUs and law enforcement agencies are able to, and

[173] Financial intelligence refers to the product resulting from analysis or work done to add value to available and obtainable information. In the case of the FIU, Financial Intelligence is the product of its operational and strategic analysis.

do seek appropriate financial and law enforcement intelligence and other information from their foreign counterparts.

4 Assessors should consider the collection of, and timely access to reported and other information, the production of financial intelligence and the use thereof across the range of relevant authorities in a country, including the FIU. While assessors should consider the production of financial intelligence across the range of relevant authorities according to the specific approach to producing financial intelligence taken by each jurisdiction, the role of the FIU should remain central.

5 When assessing the core issues below, assessors should consider the ML/TF risks in the assessed country and whether the activities conducted by the FIU and other competent authorities are aligned with the identified risks.

Core Issues to be considered in determining if the Outcome is being achieved

6.1. To what extent does the FIU access a broad range of reports, data and other information (STRs received[174] cash transaction reports,[175] cross-border declarations or disclosures on currency and bearer negotiable instruments and other sources of information)[176] to perform its functions? To what extent do other competent authorities access a broad range of reports, data and other information (including information from STRs, where allowed by national legislation) to perform their functions? Do these reports and information sources contain relevant, accurate and up to date data, and does the FIU and other relevant competent authorities have timely access to them?

6.2 To what extent is the FIU producing and disseminating financial intelligence to support the operational needs of competent authorities? Where relevant, to what extent are other competent authorities also producing financial intelligence using accessible FIU data and other relevant information that support their needs?

174 In line with R.29, FIUs are and should remain the national centre for the receipt and analysis of STRs related to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis.

175 Where required by national legislation.

176 Sources can include financial, administrative, law enforcement and open source information such as information derived from STRs, cross-border declarations or disclosures on currency and bearer negotiable movements, law enforcement intelligence; criminal records; supervisory and regulatory information; and information with company registries etc. Where applicable, it would also include reports on cash transactions, foreign currency transactions, wire transfers records, information from other government agencies including security agencies; tax authorities, asset registries, benefit agencies and information which can be obtained through compulsory measures from financial institutions; DNFBPs and VASPs including CDD information and transaction records, as well as information from open sources.

6.3 To what extent do the FIU and other competent authorities co-operate and exchange financial intelligence and information? How securely do the FIU and other competent authorities protect the confidentiality of the information they exchange or use (including financial intelligence disseminated to competent authorities by the FIU)?

6.4. To what extent do competent authorities use financial intelligence and other relevant information in investigations to develop evidence, identify assets and trace criminal proceeds or instrumentalities related to ML, associated predicate offences and TF?

a) Examples of Information that could support the conclusions on Core Issues

1 Information on STRs (e.g., *number of STRs/cases analysed; perception of quality of information disclosed in STRs; frequency with which competent authorities come across examples of unreported suspicious transactions; cases of tipping-off; see also Immediate Outcome 4 for information on STR reporting).*

2 Information on other financial intelligence and information (e.g., *number of currency and bearer negotiable instruments reports received, and analysed; types of information that law enforcement and other competent authorities receive or obtain/access from other authorities, financial institutions and DNFBPs).*

3 Examples of the co-operation between FIUs and other competent authorities and use of financial intelligence (e.g. *statistics of financial intelligence disseminated/exchanged; cases where financial intelligence was used in investigation and prosecution of ML/TF and associated predicate offences, or in identifying and tracing assets; joint task forces; shared databases; secondments).*

4 Experiences of law enforcement and other competent authorities (e.g., *types of financial intelligence and other information available; frequency with which they are used as investigative tools).*

5 Other documents (e.g., *guidance on the use and reporting of STRs and other financial intelligence; typologies produced using financial intelligence*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

6 How well does the FIU access and use additional information to analyse and add value to STRs? How well do other competent authorities access and use additional information to analyse and add value to financial intelligence information that they received, including to the analysis disseminated to them by the FIU?

7 How does the FIU ensure the rigour of its analytical assessments?

8 How well do competent authorities make use of the information contained in STRs and other financial intelligence to develop operational and strategic analysis?

9 To what extent does the FIU incorporate feedback from competent authorities, typologies and operational experience into its functions?

10 What are the mechanisms (e.g. joint task forces; shared databases; secondments) implemented to ensure full and timely co-operation between competent authorities, and from financial institutions, DNFBPs and other reporting entities to provide the relevant information? Are there any impediments to the access of information?

11 To what extent do the STRs reported contain complete, accurate and adequate information relating to the suspicious transaction?

12 To what extent do the relevant competent authorities review and engage (including outreach by the FIU) reporting entities to enhance financial intelligence reporting?

13 Do the relevant authorities have adequate skills and resources (including IT tools for data mining and analysis of financial intelligence and to protect its confidentiality) to perform its functions?

14 What are the measures implemented to ensure that the FIU has the operational independence and autonomy to carry out its functions and not be subject to undue influence on AML/CFT matters?

Immediate Outcome 7	Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.

Characteristics of an effective system

Money laundering activities, and in particular major proceeds-generating offences, are investigated; offenders are successfully prosecuted; and the courts apply effective, proportionate and dissuasive sanctions to those convicted. This includes pursuing parallel financial investigations and cases where the associated predicate offences occur outside the country, and investigating and prosecuting stand-alone money laundering offences. The component parts of the systems (investigation, prosecution, conviction, and sanctions) are functioning coherently to mitigate the money laundering risks. Ultimately, the prospect of detection, conviction, and punishment dissuades potential criminals from carrying out proceeds generating crimes and money laundering.

This outcome relates primarily to Recommendations 3, 30 and 31, and also elements of Recommendations 1, 2, 15, 32, 37, 39 and 40.

Note to Assessors:

1 Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: competent *authorities, country, foreign counterparts, legal persons, money laundering offence, proceeds, risk,* and *should*.

2 Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent to which law enforcement agencies are seeking appropriate assistance from their foreign counterparts in cross-border money laundering cases.

3 When assessing the core issues below, assessors should consider whether activities and measures are aligned with risk, including but not limited to (a) overall level of ML risk, (b) laundering related to high-risk predicate offences, (c) the characteristics of the ML activity/prosecution (stand-alone, third-party, self-laundering, complex ML, etc.),[177] (d) ML

[177] **Third party money laundering** is the laundering of proceeds by a person who was not involved in the commission of the predicate offence. **Self-laundering** is the laundering of proceeds by a person who was involved in the commission of the predicate offence. **Stand-alone (or autonomous) money laundering** is not a type of laundering, but rather refers to the prosecution of ML offences independently, without also necessarily prosecuting the predicate offence. This could be particularly relevant inter alia i) when there is insufficient evidence of the particular predicate offence that gives rise to the criminal proceeds; or ii) in situations where there is a lack of territorial jurisdiction over

methods, techniques and trends, and (e) the extent of ML based on foreign vs. domestic predicates.[178]

Core Issues to be considered in determining if the Outcome is being achieved

7.1. How well, and in what circumstances is ML activity identified and investigated (including through parallel financial investigations)?

7.2. To what extent is ML activity (including different types of ML cases) being prosecuted[179] and offenders convicted?[180]

7.3. To what extent are the sanctions applied against natural or legal persons convicted of ML offences effective, proportionate and dissuasive?

7.4. To what extent do countries apply other criminal justice measures in cases where a ML investigation has been pursued but where it is not possible, for justifiable reasons, to secure a ML conviction? Such alternative measures should not diminish the importance of, or be a substitute for, prosecutions and convictions for ML offences.

a) Examples of Information that could support the conclusions on Core Issues

1 Experiences and examples of identification, investigations, prosecutions and convictions *(* e.g., *sources of ML investigations (such as parallel financial investigations, suspicious transaction reports, open source information, domestic and foreign intelligence, etc.); examples of cases rejected due to insufficient investigative evidence; what are the significant or complex ML cases that the country has investigated and prosecuted; examples of cases that align with the country's ML risk; examples of successful cases against domestic and transnational organised crime; cases where other criminal sanctions or measures are pursued instead of ML convictions (e.g. deferred prosecution agreements with legal persons; alternative criminal offences (such as illicit enrichment or cash smuggling); etc.).*

2 Information on ML investigations, prosecutions and convictions (e.g., *number of investigations and* prosecutions *for ML activity; proportion of cases leading to prosecution or brought to court; number or proportion of ML convictions relating to third party laundering, stand-alone offence, self-laundering, and foreign predicate offences; types of predicate crimes involved; level of sanctions*

the predicate offence. The proceeds may have been laundered by the defendant (self-laundering) or by a third party (third party ML).

178 In line with paragraph 72, assessors should take into account the assessed country's national framework and legal system (including, e.g., whether the country implements a mandatory or discretionary approach to investigations and/or prosecutions).

179 I.e. The stage where an indictment has been filed.

180 When considering how well ML activity is being prosecuted, assessors should consider the types of ML cases prosecuted.

imposed for ML offences; sanctions imposed for ML compared with those for comparable economic offences (e.g., fraud, embezzlement, etc.)).

b) Examples of Specific Factors that could support the conclusions on Core Issues

3 What are the measures taken to identify, initiate and prioritise ML cases (at least in relation to all major proceeds-generating offences) for investigation (*e.g.,* focus between small and larger or complex cases, between domestic and foreign predicates etc.)?

4 To what extent, and how quickly, can competent authorities obtain or access relevant financial intelligence and other information required for ML investigations?

5 To what extent are joint or cooperative investigations (including the use of multi-disciplinary investigative units) and other investigative techniques (*e.g.,* postponing or waiving the arrest or seizure of money for the purpose of identifying persons involved) used in major proceeds generating offences?

6 How are ML cases prepared for timely prosecution and trial?

7 In what circumstances are decisions made not to proceed with prosecutions where there is indicative evidence of a ML offence?

8 To what extent are ML prosecutions: (i) linked to the prosecution of the predicate offence (including foreign predicate offences), or (ii) prosecuted as an autonomous offence?

9 How do the relevant authorities, taking into account the legal systems, interact with each other throughout the life-cycle of a ML case, from the initiation of an investigation, through gathering of evidence, referral to prosecutors and the decision to go to trial?

10 Are there other aspects of the investigative, prosecutorial or judicial process that impede or hinder ML prosecutions and sanctions?

11 Do the competent authorities have adequate resources (including financial investigation tools) to manage their work or address the ML risks adequately?

12 Are dedicated staff/units in place to investigate ML? Where resources are shared, how are ML investigations prioritised?

Immediate Outcome 8	Proceeds and instrumentalities of crime are confiscated.

Characteristics of an effective system

Criminals are deprived (through timely use of provisional and confiscation measures) of the proceeds and instrumentalities of their crimes (both domestic and foreign) or of property of an equivalent value. Confiscation includes proceeds recovered through criminal, civil or administrative processes; confiscation arising from false cross-border disclosures or declarations; and restitution to victims (through court proceedings). The country manages seized or confiscated assets, and repatriates or shares confiscated assets with other countries. Ultimately, this makes crime unprofitable and reduces both predicate crimes and money laundering.

This outcome relates primarily to Recommendations 1, 4, 32 and also elements of Recommendations 15, 30, 31, 37, 38, and 40.

Note to Assessors:

1) Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: *bearer negotiable instruments, competent authorities, confiscation, country, currency, foreign counterparts, freeze, proceeds, property, risk, seize, should*, and *terrorist financing (TF)*.

2) Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent which law enforcement and prosecutorial agencies are seeking appropriate assistance from their foreign counterparts in relation to cross-border proceeds and instrumentalities of crime.

Core Issues to be considered in determining if the Outcome is being achieved

8.1. To what extent is confiscation of criminal proceeds, instrumentalities and property of equivalent value pursued as a policy objective?

8.2. How well are the competent authorities confiscating102 (including repatriation, sharing and restitution) the proceeds and instrumentalities of crime, and property of an equivalent value, involving domestic and foreign predicate offences and proceeds which have been moved to other countries?

8.3. To what extent is confiscation regarding falsely / not declared or disclosed cross-border movements of currency and bearer negotiable instruments being addressed and applied as an effective, proportionate and dissuasive sanction by border/custom or other relevant authorities?

8.4. How well do the confiscation results reflect the assessments(s) of ML/TF risks and national AML/CFT policies and priorities?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences and examples of confiscation proceedings *(e.g., the most significant cases in the past; types of confiscation orders obtained by the country; trends indicating changes in methods by which proceeds of crime is being laundered).*
2. Information on confiscation (*e.g., number of criminal cases where confiscation is pursued; type of cases which involve confiscation; value of proceeds of crimes, instrumentalities or property of equivalent value confiscated, broken down by foreign or domestic offences, whether through criminal or civil procedures (including non-conviction-based confiscation*); value of falsely / not declared or disclosed cross-border currency and bearer negotiable instruments confiscated; value or proportion of seized or frozen proceeds that is subject to confiscation; value or proportion of confiscation orders realised).
3. Other relevant information (*e.g. value of criminal assets seized / frozen; amount of proceeds of crime restituted to victims, shared or repatriated).*

b) Examples of Specific Factors that could support the conclusions on Core Issues

4. What are the measures and approach adopted by competent authorities to target proceeds and instrumentalities of crime (including major proceeds-generating crimes and those that do not originate domestically or have flowed overseas)?
5. How do authorities decide, at the outset of a criminal investigation, to commence a financial investigation, with a view to confiscation?
6. How well are competent authorities identifying and tracing proceeds and instrumentalities of crimes or assets of equivalent value? How well are provisional measures (*e.g., freeze or seizures*) used to prevent the flight or dissipation of assets?
7. What is the approach adopted by the country to detect and confiscate cross-border currency and bearer negotiable instruments that are suspected to relate to ML/TF and associated predicate offences or that are falsely / not declared or disclosed?
8. What are the measures adopted to preserve and manage the value of seized/confiscated assets?
9. Are there other aspects of the investigative, prosecutorial or judicial process that promote or hinder the identification, tracing and confiscation of proceeds and instrumentalities of crime or assets of equivalent value?
10. Do the relevant competent authorities have adequate resources to perform their functions adequately?

Immediate Outcome 9	Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.

Characteristics of an effective system

Terrorist financing activities are investigated; offenders are successfully prosecuted; and courts apply effective, proportionate and dissuasive sanctions to those convicted. When appropriate, terrorist financing is pursued as a distinct criminal activity and financial investigations are conducted to support counter terrorism investigations, with good co-ordination between relevant authorities. The components of the system (investigation, prosecution, conviction and sanctions) are functioning coherently to mitigate the terrorist financing risks. Ultimately, the prospect of detection, conviction and punishment deters terrorist financing activities.

This outcome relates primarily to Recommendations 5, 30, 31 and 39, and also elements of Recommendations 1, 2, 15, 32, 37 and 40.

Note to Assessors*:*

1) Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: *bearer negotiable instruments, competent authorities, country, criminal activity, designation, foreign counterparts, funds or other assets, legal persons, risk, should, terrorist, terrorist financing (TF), terrorist financing offence*, and *terrorist organisation*.

2) Assessors should be aware that some elements of this outcome may involve material of a sensitive nature (*e.g.,* information that is gathered for national security purposes) which countries may be reluctant or not able to make available to assessors.

3) Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent which law enforcement and prosecutorial agencies are seeking appropriate assistance from their foreign counterparts in cross-border terrorist financing cases.

4) When assessing the core issues below, assessors should consider whether activities and measures are aligned with risk, including but not limited to (a) overall level of TF risks, (b) the characteristics of the domestic and cross-border TF activity (*e.g.,* collection, movement and

use of funds or other assets), and (c) the country's prevailing TF methods, techniques and trends.[181]

Core Issues to be considered in determining if the Outcome is being achieved

9.1 How well and in what circumstances is TF activity identified and investigated? To what extent do the investigations identify the specific role played by the terrorist financier?

9.2 To what extent is TF activity (including different types of TF cases) prosecuted and offenders convicted?[182]

9.3 To what extent are the sanctions or measures applied against natural and legal persons convicted of TF offences effective, proportionate and dissuasive?

9.4 To what extent is the investigation, prosecution and conviction of TF considered, and used, in the formulation of national counter-terrorism strategies? How well is information and intelligence obtained in TF investigations, prosecutions and convictions shared and used to support national counter-terrorism purposes and activities (*e.g.,* identification and designation of terrorists, terrorist organisations and terrorist support networks)?

9.5. To what extent is the objective of the outcome achieved by employing other criminal justice, regulatory or other measures to disrupt TF activities where it is not practicable to secure a TF conviction?[183]

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences and examples of TF identification, investigations, prosecutions and convictions (e.g., *sources of TF investigations (such as parallel financial investigations, suspicious transaction reports, open source information, domestic and foreign intelligence, etc.); cases where TF investigations are used to support counter-terrorism investigations and prosecutions; significant cases where (foreign or domestic) terrorists and terrorist groups are targeted, prosecuted or disrupted; observed trends in TF levels and techniques; cases where other criminal sanctions or measures are pursued instead of TF convictions, e.g. restrictions on activities, alternative criminal offences, etc.).*

---

181 In line with paragraph 73, assessors should take into account the assessed country's national framework and legal system (including, e.g., whether the country implements a mandatory or discretionary approach to investigations and/or prosecutions).

182 The focus of this core issue is on the prosecution and conviction of offences covered under Recommendation 5. The use of non-TF offences to pursue TF offenders should be considered in core issue 9.5. Assessors should also take into consideration the types of TF cases prosecuted.

183 This core issue may include consideration of the assessed jurisdiction's use of non-TF offences or other measures to pursue TF offenders. However, this should be distinguished from circumstances where a jurisdiction uses financial intelligence or information to pursue suspected terrorists, but does not identify, investigate or disrupt TF activity. The assessed country should demonstrate why TF prosecution was not practicable.

2. Information on TF investigations, prosecutions and convictions (e.g., *number of TF investigations and prosecutions; proportion of cases leading to TF prosecution, type of TF prosecutions and convictions (*e.g., *distinct offences, foreign or domestic terrorists, financing of the travel of foreign terrorist fighters); level of sanctions imposed for TF offences; sanctions imposed for TF compared with those for other comparable criminal activity; types and level of disruptive measures applied*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

3. What are the measures taken to identify, initiate and prioritise TF cases to ensure prompt investigation and action against major threats and to maximise disruption?

4. To what extent and how quickly can competent authorities obtain and access relevant financial intelligence and other information required for TF investigations and prosecutions?

5. What are the underlying considerations for decisions made not to proceed with prosecutions for a TF offence?

6. To what extent do the authorities apply specific action plans or strategies to deal with particular TF threats and trends? Is this consistent with the national AML/CFT policies, strategies and risks?

7. How well do law enforcement authorities, the FIU, counter-terrorism units and other security and intelligence agencies co-operate and co-ordinate their respective tasks associated with this outcome?

8. Are there other aspects of the investigative, prosecutorial or judicial process that impede or hinder TF prosecutions, sanctions or disruption?

9. Do the competent authorities have adequate resources (including financial investigation tools) to manage their work or address the TF risks adequately?

10. Are dedicated staff/units in place to investigate TF? Where resources are shared, how are TF investigations prioritised?

Immediate Outcome 10	Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds

Characteristics of an effective system

Terrorists, terrorist organisations and terrorist financiers are identified and deprived of the resources and means to finance or support terrorist activities and organisations. This includes proper implementation of targeted financial sanctions against persons and entities designated by the United Nations Security Council and under applicable national or supra-national sanctions regimes. The country also has a good understanding of the terrorist financing risks and takes appropriate and proportionate actions to mitigate those risks. These include focused, proportionate and risk-based measures that prevent the raising and moving of funds through NPOs or methods which are at risk of being misused by terrorists, without unduly disrupting or discouraging legitimate NPO activities. Ultimately, this reduces terrorist financing flows, which would prevent terrorist acts.

This outcome relates primarily to Recommendations 1, 4, 6 and 8, and also elements of Recommendations 14, 15, 16, 26, 30 to 32, 35, 37, 38 and 40.

Note to Assessors:

1) Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: *accounts, appropriate authorities, competent authorities, country, designated non-financial businesses and professions (DNFBP); designated person or entity, designation, financial group, financial institutions, freeze, funds, funds or other assets, non-profit organisations (NPO), risk, seize, self-regulatory measures, should, targeted financial sanctions, terrorist, terrorist act, terrorist financing (TF), terrorist financing abuse, terrorist organisation,* and *without delay*.
2) When assessing core issues 10.2 to 10.5, assessors should consider whether activities and measures are aligned with TF risk, including but not limited to (a) the overall level of TF risks, (b) the characteristics of the domestic and cross-border TF activity (*e.g.,* collection, movement and use of funds or other assets), and (c) the country's prevailing TF methods, techniques and trends.
3) Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome.

Core Issues to be considered in determining if the Outcome is being achieved

10.1. How well is the country implementing, without delay, targeted financial sanctions pursuant to (i) UNSCR1267 and its successor resolutions, and (ii) UNSCR1373 (at the supra-national or national level, whether on the country's own motion or after examination, to give effect to the request of another country)?

10.2. To what extent are the funds and other assets of terrorists, terrorist organisations and terrorist financiers, including designated persons and entities and those acting on their behalf or at their direction, being identified? To what extent are such persons and entities prevented from raising, moving and using funds or other assets, including by operating or executing financial transactions?

10.3. To what extent, without unduly disrupting or discouraging legitimate NPO activities, has the country applied focused, proportionate and risk-based mitigation measures to only those organisations which fall within the FATF definition of NPOs, in line with identified TF risk?

10.4. To what extent do financial institutions, DNFBPs and VASPs comply with and understand their obligations regarding targeted financial sanctions relating to financing of terrorism and terrorist organisations?

10.5. How well are relevant competent authorities monitoring and ensuring compliance[184] by financial institutions, DNFBPs and VASPs with their obligations regarding targeted financial sanctions relating to financing of terrorism and terrorist organisations?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences of law enforcement, FIU and counter terrorism authorities (e.g., *trends indicating that terrorist financiers are researching alternative methods for raising / transmitting funds; intelligence/source reporting indicating that terrorist organisations are having difficulty raising funds in the country*).

2. Examples of interventions (e.g., *significant cases where terrorists, terrorist organisations or terrorist financiers are prevented from raising, moving and using funds or their assets seized / confiscated; investigations and interventions in NPOs misused by terrorists).*

3. Information on targeted financial sanctions (e.g., *persons and accounts subject to targeted financial sanctions under UNSC or other designations; designations made (relating to UNSCR 1373); assets frozen; transactions rejected; time taken to designate individuals; time taken to implement asset freeze following designation*).

4. Information on sustained outreach and targeted risk-based supervision and monitoring of NPOs that the country has identified as being at risk of terrorist financing abuse (*e.g. frequency of review and monitoring of such NPOs (including risk assessments); frequency of*

[184] In line with the requirements for supervisors, ensuring compliance includes providing outreach, training and applying remedial actions and/or effective, proportionate and dissuasive sanctions where appropriate, as well as assessing their positive impact on compliance by financial institutions, DNFBP's and VASPs?

engagement and outreach (including guidance) to NPOs regarding CFT measures and trends; remedial measures and sanctions taken against NPOs).

b) Examples of Specific Factors that could support the conclusions on Core Issues

5. What measures has the country adopted to ensure the proper implementation of targeted financial sanctions without delay? How are those designations and obligations communicated to financial institutions, DNFBPs, VASPs and the general public in a timely manner?

6. How well are the procedures and mechanisms implemented for (i) identifying targets for designation / listing, (ii) freezing / unfreezing, (iii) de-listing, and (iv) granting exemption? How well is the relevant information collected?

7. To what extent is the country utilising the tools provided by UNSCRs 1267 and 1373 to freeze and prevent the financial flows of terrorists?

8. How well do the systems for approving or licensing the use of assets by designated entities for authorised purposes comply with the requirements set out in the relevant UNSCRs?

9. What is the approach adopted by competent authorities to target terrorist assets? To what extent are assets tracing, financial investigations and provisional measures (*e.g.,* freezing and seizing) used to complement the approach?

10. To what extent does the country understand the level of risk of organisations that fall within the FATF definition of NPO and the nature of TF threats posed to them?

11. For NPOs identified as low risk of TF abuse, to what extent is the country's level of outreach consistent with the level of identified risk?

12. For NPOs other than those identified to be at low risk, to what extent are all four of the following elements being used to identify, prevent and combat terrorist financing abuse of NPOs without unduly disrupting or discouraging legitimate NPO activities: (a) sustained outreach, (b) targeted risk-based oversight or monitoring, (c) effective investigation and information gathering, and (d) effective mechanisms for international co-operation? To what extent are the measures being applied focused proportionate and risk-based?

13. To what extent are appropriate investigative, criminal, civil or administrative actions, co-operation and co-ordination mechanisms applied to NPOs suspected of being exploited by, or actively supporting terrorist activity or terrorist organisations? Do the appropriate authorities have adequate resources to perform their outreach / oversight / monitoring / investigation duties effectively?

14. How well do NPOs understand the nature of TF threats posed to them and apply measures to protect themselves from the threat of terrorist abuse?

15. Are there other aspects of the investigative, prosecutorial, judicial or other processes that promote or hinder: (a) the identification of funds or other assets related to terrorists, terrorist organisations or terrorist financiers, or (b) measures that prevent such persons or entities from raising, moving and using funds or other assets?

16. What measures and supervisory tools are employed to ensure that financial institutions and VASPs (including financial groups), as well as DFNBPs (including groups as appropriate), are regulated and comply with their obligations which relate to targeted financial sanctions on terrorism?

17. Do the relevant competent authorities, including those responsible for oversight, monitoring and investigation of NPOs, have adequate resources to manage their work or address the terrorist financing risks adequately

18. Where resources are shared, how are terrorist financing related activities prioritised?

Immediate Outcome 11	Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

Characteristics of an effective system

Persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMD) are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation. Targeted financial sanctions are fully and properly implemented without delay; monitored for compliance. There is adequate co-operation and co-ordination between the relevant authorities to develop and implement policies and activities to combat the financing of proliferation of WMD. Risks of potential breaches, non-implementation or evasion of targeted financial sanctions obligations are identified, assessed and understood and risk-based measures to mitigate these risks are applied to strengthen implementation of targeted financial sanctions.

This outcome relates to Recommendation 7 and elements of Recommendations 1, 2 and 15.

Note to Assessors*:*

1) Assessors should refer to the following Glossary definitions when assessing this Immediate Outcome: *accounts, beneficial owner, competent authorities, country, designated non-financial* businesses *and professions (DNFBP); designated person or entity, designation, financial institutions, freeze, funds, funds or other assets, legal persons, property, risk, should, targeted financial sanctions*, and *without delay.*

2) When assessing core issue 11.2, assessors are not expected to re-assess the country's assessment(s) of PF risks.[185] Assessors, based on their views of the reasonableness of the assessment(s) of risks, and taking into account the context of the country, as set out in paragraphs 5-13 of the Methodology, should focus on how well the competent authorities have identified, assessed and understood the PF risks facing the country.

185 "Proliferation financing risk" refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.

Core Issues to be considered in determining if the Outcome is being achieved

11.1. To what extent do the competent authorities co-operate and co-ordinate the development and implementation of policies,[186] and, for operational purposes co-operate and, where appropriate, co-ordinate to combat financing of proliferation of weapons of mass destruction?[187]

11.2 How well does the country identify, assess, and understand and mitigate the risk of potential breaches, non-implementation- or evasion of obligations regarding targeted financial sanctions relating to financing of proliferation present in the country in both higher and lower risk scenarios?

11.3 How well is the country implementing, without delay, targeted financial sanctions concerning the UNSCRs relating to the combating of financing of proliferation?

11.4 To what extent are the funds or other assets of designated persons and entities and those acting on their behalf or at their direction identified and such persons and entities prevented from operating or from executing financial transactions related to proliferation?

11.5. To what extent do financial institutions, DNFBPs and VASPs comply with, and understand their obligations regarding targeted financial sanctions relating to financing of proliferation? [188]

11.6. How well are relevant competent authorities monitoring and ensuring compliance by financial institutions, DNFBPs and VASPs with their obligations regarding targeted financial sanctions relating to financing of proliferation?

a) Examples of Information that could support the conclusions on Core Issues

1. Examples of investigations and intervention relating to financing of proliferation (e.g., *investigations into breaches of sanctions; significant cases in which country has taken enforcement actions* (e.g., *freezing or seizures) or provided assistance).*

2. Information on targeted financial sanctions relating to financing of proliferation (e.g., *accounts of individuals and entities subject to targeted financial sanctions; value of frozen assets and property; time taken to designate persons and entities; time taken to freeze assets and property of individuals and entities following their designation by the UNSC*).

3. The country's assessment(s) of its risks of potential breaches, non-implementation or evasion of targeted financial sanctions obligations relating to financing of proliferation present in the country and related policies and strategies (e.g., *types of assessment(s) produced; types of*

186 Having regard to requirements and Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation) as needed.

187 Considering that there are different forms of co-operation and co-ordination between relevant authorities, core issue 11.1 does not prejudge a country's choice for a particular form and applies equally to all of them.

188 For the purposes of core issues 11.3 and 11.4, this includes the obligation to understand their risks of potential breaches, non-implementation or evasion of targeted financial sanctions obligations relating to financing of proliferation and take risk-based measures to mitigate the risks identified as outlined in Recommendation 1.

assessment(s), policies, strategies and statements published / communicated; engagement and commitment at the senior officials and political level).

4. Information on engagement of relevant authorities at policy and operational levels (*e.g. frequency and relevancy of engagement on policies and legislation; use of both formal and informal communication and co-operation channels frameworks and mechanisms; cases of successful inter-agency co-ordination).*

5. Monitoring and other relevant information relating to financing of proliferation, including information on risk of potential breaches, non-implementation or evasion of targeted financial sanctions obligations relating to financing of proliferation (*e.g., frequency of review and monitoring of financial institutions, DNFBPs and VASPs for compliance with targeted financial sanctions; frequency of engagement and outreach; guidance documents; level of sanctions applied on financial institutions, DNFBPs* and VASPs *for breaches*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

6. What measures has the country adopted to ensure the proper implementation of targeted financial sanctions relating to financing of proliferation without delay? How are these designations and obligations communicated to relevant sectors in a timely manner?

7. Where relevant, how well are the procedures implemented for (i) designation / listing, (ii) freezing / unfreezing, (iii) de-listing, and (iv) granting exemption? To what extent do they comply with the UNSCR requirements?

8. How well do the systems and mechanisms for managing frozen assets and licensing the use of assets by designated individuals and entities for authorised purposes, safeguard human rights and prevent the misuse of funds?

9. What are the methods, tools, and information used to develop, review and evaluate the conclusions of the assessment(s) of risks of potential breaches, non-implementation or evasion of targeted financial sanctions obligations relating to financing of proliferation? How comprehensive are the information and data used?

10. What mechanisms are used to prevent the potential breaches, non-implementation or evasion of sanctions? Are they commensurate with the identified level of risks of potential breaches, non-implementation or evasion of targeted financial sanctions obligations? Do relevant competent authorities provide financial institutions, DNFBPs and VASPs with other guidance or specific feedback?

11. What mechanism(s) or body do the authorities use to ensure proper and regular co-operation and co-ordination of the national framework, including timely sharing of relevant information and development and implementation of policies to combat the financing of proliferation of weapons of mass destruction, at both policymaking and operational levels? Does the mechanism or body include all relevant authorities?

12. To what extent would the relevant competent authorities be able to obtain accurate basic and beneficial ownership information on legal persons (*e.g.,* front companies), when investigating offences or breaches concerning the UNSCRs relating financing of proliferation?

13. To what extent are the relevant competent authorities exchanging intelligence and other information for assessing risks, and conducting investigations of violations and breaches of targeted financial sanctions in relation to financing of proliferation, as per the relevant UNSCRs?

14. Do the relevant competent authorities have adequate resources to manage their work or address the financing of proliferation risks adequately?

GENERAL GLOSSARY

Terms	Definitions
Accounts	References to "accounts" should be read as including other similar business relationships between financial institutions and their customers.
Accurate	Please refer to the IN to Recommendation 16.
Agent	For the purposes of Recommendations 14 and 16, *agent* means any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.
Appropriate authorities	Please refer to the IN to Recommendation 8.
Associate NPOs	Please refer to the IN to Recommendation 8.
Batch transfer	Please refer to the IN to Recommendation 16.
Bearer negotiable instruments	*Bearer negotiable instruments (BNIs)* includes monetary instruments in bearer form such as: traveller's cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.
Bearer shares	*Bearer shares* refers to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.
Beneficial owner	*Beneficial owner* refers to the natural person(s) who ultimately[189] owns or controls a customer[190] and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiaries	Please refer to the IN to Recommendation 8.

[189] Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

[190] This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

Terms	Definitions
Beneficiary	The meaning of the term *beneficiary* in the FATF Recommendations depends on the context: ■ In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally coextensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. ■ In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy. Please also refer to the Interpretive Notes to Recommendation 16.
Beneficiary Financial Institution	Please refer to the IN to Recommendation 16.
Competent authorities	*Competent authorities* refers to all public authorities [191] with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as competent authorities.

[191] This includes financial supervisors established as independent non-governmental authorities with statutory powers.

Terms	Definitions
Confiscation	The term *confiscation,* which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.
Core Principles	*Core Principles* refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Correspondent banking	*Correspondent banking* is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
Country	All references in the FATF Recommendations to *country* or *countries* apply equally to territories or jurisdictions.
Cover Payment	Please refer to the IN. to Recommendation 16.
Criminal activity	*Criminal activity* refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3.
Cross-border Wire Transfer	Please refer to the IN to Recommendation 16.
Currency	*Currency* refers to banknotes and coins that are in circulation as a medium of exchange.

Terms	Definitions
Designated categories of offences	*Designated categories of offences* means: ■ participation in an organised criminal group and racketeering; ■ terrorism, including terrorist financing; ■ trafficking in human beings and migrant smuggling; ■ sexual exploitation, including sexual exploitation of children; ■ illicit trafficking in narcotic drugs and psychotropic substances; ■ illicit arms trafficking; ■ illicit trafficking in stolen and other goods; ■ corruption and bribery; ■ fraud; ■ counterfeiting currency; ■ counterfeiting and piracy of products; ■ environmental crime; (for example, criminal harvesting, extraction or trafficking of protected species of wild fauna and flora, precious metals and stones, other natural resources, or waste). ■ murder, grievous bodily injury; ■ kidnapping, illegal restraint and hostage-taking; ■ robbery or theft; ■ smuggling; (including in relation to customs and excise duties and taxes); ■ tax crimes (related to direct taxes and indirect taxes); ■ extortion; ■ forgery; ■ piracy; and ■ insider trading and market manipulation. When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

Terms	Definitions
Designated nonfinancial businesses and professions	*Designated non-financial businesses and professions* means: a Casinos;[192] b Real estate agents; c Dealers in precious metals; d Dealers in precious stones; e Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures;
	f Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: ■ acting as a formation agent of legal persons; ■ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; ■ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; ■ acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; ■ acting as (or arranging for another person to act as) a nominee shareholder for another person.

[192] References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

Terms	Definitions
Designated person or entity	The term designated person or entity refers to: i individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida; ii individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; iii any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001); iv any individual, natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1718 (2006) and any future successor resolutions by the Security Council in annexes to the relevant resolutions, or by the Security Council Committee established pursuant to resolution 1718 (2006) (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and v any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 2231 (2015) and any future successor resolutions by the Security Council.

Terms	Definitions
Designation	The term *designation* refers to the identification of a person,[193] individual or entity that is subject to targeted financial sanctions pursuant to: ■ United Nations Security Council resolution 1267 (1999) and its successor resolutions; ■ Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination; ■ Security Council resolution 1718 (2006) and any future successor resolutions; ■ Security Council resolution 2231 (2015) and any future successor resolutions; and ■ any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. As far as Security Council resolution 2231 (2015) and any future successor resolutions are concerned, references to "designations" apply equally to "listing".
Domestic Wire Transfer	Please refer to the IN to Recommendation 16.
Enforceable means	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Ex Parte	The term *ex parte* means proceeding without prior notification and participation of the affected party.
Express trust	*Express trust* refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).
False declaration	Please refer to the IN to Recommendation 32.

[193] Natural or legal.

Terms	Definitions
False disclosure	Please refer to the IN to Recommendation 32.
Financial group	*Financial group* means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Financial institutions	*Financial institutions* means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1 Acceptance of deposits and other repayable funds from the public.[194] 2 Lending.[195] 3 Financial leasing.[196] 4 Money or value transfer services.[197] 5 Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6 Financial guarantees and commitments. 7 Trading in: *a* money market instruments (cheques, bills, certificates of deposit, derivatives etc.); *b* foreign exchange; *c* exchange, interest rate and index instruments; *d* transferable securities; *e* commodity futures trading. 8 Participation in securities issues and the provision of financial services related to such issues.

194 This also captures private banking.

195 This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

196 This does not extend to financial leasing arrangements in relation to consumer products.

197 It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.

Terms	Definitions
	9 Individual and collective portfolio management. 10 Safekeeping and administration of cash or liquid securities on behalf of other persons. 11 Otherwise investing, administering or managing funds or money on behalf of other persons. 12 Underwriting and placement of life insurance and other investment related insurance;[198] 13 Money and currency changing.
Foreign counterparts	Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the co-operation which is sought, even where such foreign competent authorities have a different nature or status (e.g. depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).

198 This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Terms	Definitions
Freeze	In the context of confiscation and provisional measures (e.g., Recommendations 4, 32 and 38), the term freeze means to prohibit the transfer, conversion, disposition or movement of any property, equipment or other instrumentalities on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism, or until a forfeiture or confiscation determination is made by a competent authority. For the purposes of Recommendations 6 and 7 on the implementation of targeted financial sanctions, the term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security Council or in accordance with applicable Security Council resolutions by a competent authority or a court. In all cases, the frozen property, equipment, instrumentalities, funds or other assets remain the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such natural or legal person(s) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of a freeze, countries may decide to take control of the property, equipment, instrumentalities, or funds or other assets as a means to protect against flight.
Fundamental principles of domestic law	This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.
Funds	The term *funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.

Terms	Definitions
Funds or other assets	The term *funds or other assets* means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.
Identification data	The term *identification data* refers to reliable, independent source documents, data or information.
Intermediary financial institution	Please refer to the IN to Recommendation 16.
International organisations	International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.
Law	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Legal arrangements	*Legal arrangements* refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.

Terms	Definitions
Legal persons	*Legal persons* refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.
Money laundering offence	References (except in Recommendation 3) to a *money laundering offence* refer not only to the primary offence or offences, but also to ancillary offences.
Money or value transfer service	*Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*.
Non-conviction based confiscation	*Non-conviction-based confiscation* means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required.
Non-profit organisation	Please refer to the IN to Recommendation 8.
Originator	Please refer to the IN to Recommendation 16.
Ordering financial institution	Please refer to the IN to Recommendation 16.
Payable-through accounts	Please refer to the IN to Recommendation 13.
Physical cross border transportation	Please refer to the IN. to Recommendation 32.

Terms	Definitions
Politically Exposed Persons (PEPs)	*Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. *Persons who are or have been entrusted with a prominent function by an international organisation* refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Proceeds	*Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	*Property* means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Qualifying wire transfers	Please refer to the IN to Recommendation 16.
Reasonable measures	The term *Reasonable Measures* means: appropriate measures which are commensurate with the money laundering or terrorist financing risks.
Related to terrorist financing or money laundering	Please refer to the IN. to Recommendation 32.
Required	Please refer to the IN to Recommendation 16.

Terms	Definitions
Risk	All references to *risk* refer to the risk of money laundering and/or terrorist financing. This term should be read in conjunction with the Interpretive Note to Recommendation 1.
Satisfied	Where reference is made to a financial institution being *satisfied* as to a matter, that institution must be able to justify its assessment to competent authorities.
Seize	The term *seize* means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.
Self-regulatory body (SRB)	A SRB is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.
Serial Payment	Please refer to the IN. to Recommendation 16.
Settlor	*Settlors* are natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.
Shell bank	*Shell bank* means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.
Should	For the purposes of assessing compliance with the FATF Recommendations, the word *should* has the same meaning as *must.*
Straight-through processing	Please refer to the IN. to Recommendation 16.

Terms	Definitions
Supervisors	*Supervisors* refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("*financial supervisors*")[199] and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.
Targeted financial sanctions	The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
Terrorist	The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

199 Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

Terms	Definitions
Terrorist act	A *terrorist act* includes: a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999). b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist financing	*Terrorist financing* is the financing of terrorist acts, and of terrorists and terrorist organisations.
Terrorist financing abuse	Please refer to the IN to Recommendation 8.
Terrorist financing offence	References (except in Recommendation 4) to a *terrorist financing offence* refer not only to the primary offence or offences, but also to ancillary offences.

Terms	Definitions
Terrorist organisation	The term *terrorist organisation* refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third parties	For the purposes of Recommendations 6 and 7, the term *third parties* includes, but is not limited to, financial institutions and DNFBPs. Please also refer to the IN to Recommendation 17.
Trustee	The terms *trust* and *trustee* should be understood as described in and consistent with Article 2 of the *Hague Convention on the law applicable to trusts and their recognition.*[121] Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or nonprofessional (e.g. a person acting without reward on behalf of family).
Unique transaction reference number	Please refer to the IN. to Recommendation 16.

[121] Article 2 of the Hague Convention reads as follows:

For the purposes of this Convention, the term "trust" refers to the legal relationships created – inter-vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose.

A trust has the following characteristics -

a) the assets constitute a separate fund and are not a part of the trustee's own estate;

b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee;

c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.

The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

Virtual Asset	A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations
Virtual Asset Service Providers	Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer[200] of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
Wire transfer	Please refer to the IN to Recommendation 16.
Without delay	The phrase without delay means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

200 In this context of virtual assets, *transfer* means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

LEGAL BASIS OF REQUIREMENTS ON FINANCIAL INSTITUTIONS AND DNFBPS AND VASPS

1. All requirements for financial institutions, DNFBPs or VASPs should be introduced either (a) in law (see the specific requirements in Recommendations 10, 11 and 20 in this regard), or (b) for all other cases, in law or enforceable means (the country has discretion).

2. In Recommendations 10, 11 and 20, the term "*law*" refers to any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for noncompliance. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.

3. The term "*Enforceable means*" refers to regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35).

4. In considering whether a document or mechanism has requirements that amount to *enforceable means*, the following factors should be taken into account:

   a There must be a document or mechanism that sets out or underpins requirements addressing the issues in the FATF Recommendations, and providing clearly stated requirements which are understood as such. For example:

      i if particular measures use the word *shall* or *must*, this should be considered mandatory;

      ii if they use *should*, this could be mandatory if both the regulator and the regulated institutions demonstrate that the actions are directly or indirectly required and are being implemented; language such as measures *are encouraged*, *are recommended* or institutions *should consider* is less likely to be regarded as mandatory. In any case where weaker language is used, there is a presumption that the language is not mandatory (unless the country can demonstrate otherwise).

   b The document/mechanism must be issued or approved by a competent authority.

   c There must be sanctions for non-compliance (sanctions need not be in the same document that imposes or underpins the requirement, and can be in another document, provided that there are clear links between the requirement and the available sanctions), which should be effective, proportionate and dissuasive. This involves consideration of the following issues:

i there should be an adequate range of effective, proportionate and dissuasive sanctions available if persons fail to comply with their obligations;

ii the sanctions should be directly or indirectly applicable for a failure to comply with an AML/CFT requirement. If non-compliance with an AML/CFT requirement does not have a sanction directly attached to it, then the use of sanctions for violation of broader requirements, such as not having proper systems and controls or not operating in a safe and sound manner, is satisfactory provided that, at a minimum, a failure to meet one or more AML/CFT requirements could be (and has been as appropriate) adequately sanctioned without a need to prove additional prudential failures unrelated to AML/CFT; and

iii whether there is satisfactory evidence that effective, proportionate and dissuasive sanctions have been applied in practice.

5. In all cases it should be apparent that financial institutions, DNFBPs and VASPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

ANNEX I: MUTUAL EVALUATION REPORT TEMPLATE

Notes for Assessors:

This template should be used as the basis for preparing Mutual Evaluation Reports (MERs) for evaluations conducted using the FATF's *2022 Methodology*. It sets out the structure of the MER, and the information and conclusions which should be included in each section.

The template incorporates guidance to assessors on how the MER should be written, including what information should be included, and the way analysis and conclusions should be presented. This guidance is clearly indicated in grey shaded text (like this section). It should not appear in the final MER. Text which appears in unshaded script (including chapter and section headings and pro-forma paragraphs) should be included in the final report (with any square brackets completed as necessary).

Assessors should note that a completed MER (not including the Key Recommended Action (KRA) Roadmap, Executive Summary, or Technical Compliance Annex (TC Annex)) is expected to be ideally 100 pages or less (together with a TC annex of 60 pages or less). There is no predetermined limit to the length of each chapter, and assessors may decide to devote more, or less, attention to any specific issue, as the country's situation requires. Countries with more complex AML/CFT/CPF regimes or context may require more analysis to ensure all necessary elements are covered. Nevertheless, assessors should ensure the MER does not become excessively long and should be prepared to edit their analysis as necessary. To ensure the right balance in the final report, assessors should aim to summarise technical compliance with each Recommendation in one or two paragraphs, totalling a maximum of half a page. Assessors may be very brief on issues where there is little or no substance to report (e.g. a single sentence description of technical compliance would be sufficient for Recommendations rated "compliant").

The Key Recommended Actions (KRA) Roadmap is intended to identify each country's highest priority follow-up actions and serve as the basis for each country's follow-up or ICRG process. It is therefore critical that assessors follow the guidance in that section to ensure that KRAs are drafted in a way that is practical, achievable, measurable, precise and clear, without being overly prescriptive.

The Executive Summary is intended to serve as the basis for Plenary discussion of each Mutual Evaluation, and to provide clear conclusions and recommendations for ministers, legislators, and other policymakers in the assessed country. It is therefore important that it does not exceed five pages, and that assessors follow the guidance in that section on the selection and presentation of issues.

Assessors are urged to include statistics and case studies where relevant. These should be provided in the format shown at the end of the template.

Key Recommended Actions (KRA) Roadmap

Assessors should compile the Key Recommended Actions in a separate list for the country (the KRA Roadmap) (*Universal Procedures* (*UPs*) para.88. The KRA Roadmap is a separate document that is prepared after the on-site visit at the same time as the first draft of the MER (*UPs,* para.88) and developed in close collaboration with the assessed country for the duration of the ME process.

Assessors should review the *Methodology* Introduction para. 72 to 76 for guidance on developing recommended actions, determining which will be Key Recommended Actions and other recommended actions and preparing the KRA Roadmap.

Subject to the *Methodology* Introduction para. 72, Key Recommended Actions should only relate to IOs rated ME or LE or Recommendations rated PC or NC where these relate to any IO rated ME or LE. Normally, there should be no more than two to three KRA related to each IO rated ME or LE, including KRA for technical compliance for Recommendations related to that IO. In addition, there may be one KRA for each of Recommendations 3, 5, 6, 10, 11, and 20 that is rated NC or PC, where these do not pertain to any IO rated ME or LE.

After the MER is adopted, the KRA Roadmap will be provided to the appropriate minister of the assessed country to advise the Minister of expectations for follow-up. (*UPs*, para.111)

EXECUTIVE SUMMARY

Notes for Assessors:

The Executive Summary is a separate document that is prepared after the face-to-face meeting (*UPs,* para.98).

1. This report summarises the AML/CFT measures in place in [name of assessed country] as at the date of the on-site visit [date]. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of [country]'s AML/CFT system and provides recommendations on how the system could be strengthened.

Key Findings

a) Assessors should provide a short summary of the most important key findings, both positive and negative, taking into account the country's risk profile and AML/CFT regime. The focus should be on 5-7 points raised in the report rather than a summary of the key findings for every single IO or chapter.

Effectiveness & Technical Compliance Ratings

Table 1. Effectiveness Ratings

IO.1	IO.2	IO.3	IO.4	IO.5	IO.6	IO.7	IO.8	IO.9	IO.10	IO.11

Note: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

Table 2. Technical Compliance Ratings

Assessors should indicate using green text which are the Recommendations under review (RUR) for this mutual evaluation (ME). Recommendations where the Standards have changed since the last round of mutual evaluations are already so indicated and should be assessed for every ME.

R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10
R.11	R.12	R.13	R.14	R.15	R.16	R.17	R.18	R.19	R.20
R.21	R.22	R.23	R.24	R.25	R.26	R.27	R.28	R.29	R.30
R.31	R.32	R.33	R.34	R.35	R.36	R.37	R.38	R.39	R.40

Note: Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non-compliant.

Risks and General Situation

2.

1. This section should give a brief summary (1-2 paragraphs) of the country's ML/TF risk situation and context – focusing in particular on the country's exposure to domestic and international ML/TF risks and identifying the issues and sectors that present the greatest risks. Assessors should note any areas where they have identified material risks which were not considered in the country's own risk assessment, or where they consider the level of risk to be significantly different.
2. Overall Level of Compliance and Effectiveness

3.

4. Assessors should give a very brief overview of the AML/CFT situation in the country, based on the level of both compliance and effectiveness.
5. In the sections below, assessors should briefly summarise, the overall level of effectiveness of the country's AML/CFT system in each thematic area as well as the overall level of technical compliance with the FATF Recommendations, noting any areas of particular strength or weakness. Assessors should also note the progress since the last MER, highlighting any significant changes and flagging any key issues that remain outstanding from the previous assessment.

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

6.

7. Assessors should set out their main findings in more details and for each chapter of the main report as structured in sub-sections below. Any relevant factors of importance would need to be highlighted such as high-risk or significant contextual or other issues for the country; areas where the country performs particularly well both on effectiveness and technical compliance, highlighting unusual or innovative mechanisms; significant failures of effectiveness; and important areas of technical non-compliance. Each section should contain a brief summary of the assessor's conclusions on the overall level of compliance and effectiveness – including highlighting key findings for each relevant IOs – and any actions required. The description should include sufficient detail for readers to understand assessors' conclusions and the main issues/positive features. However, it should not include a full analysis, and should not defend assessors' conclusions or anticipate and rebut objections. Any additional information should be set out in the main body of the report, rather than in the Executive Summary.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

8.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

9.

Supervision and preventive measures for FIs/VASPs and DNFBPs (Chapter 5; IO.3, 4; R.9–23, 26–28, 34 & 35)

10.

Transparency and beneficial ownership (Chapter 6; IO.5; R.24, 25)

11.

International cooperation (Chapter 7; IO.2; R.36–40)

12.

MUTUAL EVALUATION REPORT

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 on-site 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*. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from [dates].

The evaluation was conducted by an assessment team consisting of:

- [list names, agencies and countries of examiners and their role *e.g.* legal expert]
-

with the support from the FATF Secretariat of [list names from the FATF Secretariat].

The report was reviewed by [list names and countries or organisations of reviewers].

[Country] previously underwent a Mutual Evaluation in [year], conducted according to the *2013 FATF Methodology*. The [date] evaluation [*and [date] follow-up report(s)*] has [have] been published and is [are] available at [web address].

That Mutual Evaluation concluded that the country was compliant (C) with [...] Recommendations; largely compliant (LC) with [...]; partially compliant (PC) with [...]; and non-compliant (NC) with [...]. [Country] was rated C or LC with [...] of the following 5 Recommendations which were triggers for enhanced follow-up during the last round: R.3, 5, 10, 11 and 20).[201]

Based on these results, [country] was placed in [regular][enhanced] follow-up [active ICRG review]. Since its last evaluation, [country] achieved [...] technical compliance re-ratings [use the following format to list the TC re-ratings]:

- [number] Recommendations upgraded from NC to [...]: R.X, X, X;
- [number] Recommendations [upgraded][downgraded] from [...] to [...]: R.X, X, X; [...]

Based on this progress, [country] [was moved from enhanced to regular follow-up][remains in enhanced follow-up for both technical compliance and effectiveness deficiencies][remains in enhanced follow-up for technical compliance deficiencies][remains in enhanced follow-up for effectiveness deficiencies][remains in regular follow-up].

[201] 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, 5, 6, 10, 11 and 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.

In total, [number] Recommendations remain rated NC ([list them]) and [number] Recommendations ([list them])remain rated PC since the last evaluation of [country] [, including R.3, 5, 10, 11, 20 (delete as appropriate)].

CHAPTER 1. ML/TF RISKS AND CONTEXT

1.

2. Assessed countries will provide most of the information necessary to complete Chapter 1 based on the questionnaire provided in the *Universal Procedures* and on the information required to complete this template. Assessors should review that information critically to ensure that the final text of Chapter 1 is factually objective and balanced.
3. This section should begin with a very brief description of the country's general situation: its size, territorial makeup and constitutional structure.
4. This section should note any territorial or jurisdictional issues affecting the evaluation, (*e.g.* if the MER includes assessment of territories or regions with different AML/CFT regimes, or if the country is part of a supranational jurisdiction).
5. For any of the information contained in sub-sections 1.1-1.4, assessors should provide a balanced picture where possible thus covering, for example, higher risk or lower risk areas, strengths and weaknesses.
6. Assessors should remember that "property", "proceeds", "funds", "funds or other assets", or other "corresponding value" include virtual assets when assessing any Recommendation or Immediate Outcome using these terms.[202]

1.1 ML/TF Risks and Scoping of Higher-Risk Issues

1.1.1 Overview of ML/TF/PF Risks

7.

8. This section should set out the ML, TF and PF threats, vulnerabilities and risks faced by the country. It should include the main underlying threats, drawing on the risk assessment and on other relevant information, as set out in the introduction to the *Methodology*. Particular points to cover include:

- the underlying levels of proceeds generating crime in the country, its nature and the estimated value of proceeds (to the extent possible);
- the country's exposure to cross-border illicit flows (related to crimes in other countries) – including any significant potential role as a transit route for illicit goods or funds;
- any available information on the country's exposure to terrorist financing threats (including the existence of terrorist groups active in the country; or the use of the

202 See additional guidance in Introduction to the *Methodology*, para. 15 and Note to assessors at R.15.

country as a source of funds or recruits for terrorist groups active in other countries) and financing of proliferation; and

- the ML/TF/PF risks, taking into account vulnerabilities (including vulnerabilities posed by virtual asset activity) and consequences.

1.1.2 Country's risk assessment & Scoping of Higher Risk Issues

Notes for Assessors:

This section should give a high-level summary of the country risk assessment and avoid duplication of detailed information provided in R.1 and IO.1. This section should focus more on the conclusions of the enhanced risk and scoping exercise.

9.

10. The above should be framed in the context of the country's understanding and assessment of its own risks based on the information provided during the enhanced risk and scoping exercise.[203] Assessors should briefly set out any additional risks or risk factors which they consider significant, but which were not adequately taken into account in the country's risk assessment.[204] If assessors identify such additional risks, they should note the basis for their judgement, and the credible or reliable sources of information supporting this.

11. Assessors should summarise the scoping exercise conducted prior to the onsite to identify higher and lower risk issues to be considered in more detail in the course of the assessment. This should include setting out the reasons why they consider each issue to be higher or lower risk and noting how additional or less attention was given to these issues in the course of the evaluation.

1.2 Materiality

12.

13. This section should set out: the size (GDP), integration and general makeup of the economy; the amount of business which is domestic or cross-border; the extent to which the economy is cash-based (e.g. cash transactions account for what percentage of all transactions); and estimates of the size of the informal sector or shadow economy. This section should also note any other significant factors affecting materiality, as set out in paragraph 9 of the introduction to the *Methodology* including the country's population size, level of development, geographical factors, and trading, cultural and social links. It should be a brief summary.

1.2.1 Financial sector, VASPS and DNFBPs

14. In this section, assessors should describe the size and makeup of the financial sector (including the percentage of the GDP it comprises where available), generic types of virtual asset activities and providers primarily being used in the country, and

203 See *Universal Procedures*, para.57 – 62

204 When risks were not adequately taken into account in the country's risk assessment, assessors should make a cross-reference to Chapter 2, where those weaknesses should be described, to avoid duplication of text.

DNFBPs, including if the country is an international or regional financial centre. Assessors should also summarise the types and key features of financial institutions, VASPs and DNFBPs which exist in the country, and the numbers of each type of institution, as well as some information relating to the materiality of the sector and the institutions within it. Tables provided by the assessed country in the Chapter 1 questionnaire should be used to summarise the information.

15. Assessors should note (based on risk, materiality and context) the relative importance of different types of financial institutions, VASPs and DNFBPs, and their financial products and activities.[205] It is particularly important for assessors to explain their weighing of the relative importance of the different types of financial institutions, VASPs and DNFBPs to encourage consistent weighting throughout the MER, particularly when assessing IO.3 for financial institutions and VASPs and IO.4 for DNFBPs. This is important because the risks, materiality and context varies widely from country to country. For example, in some countries, a particular type of financial institution may be as (or almost as) important as the banking sector which means that weak supervision or weak preventive measures in that sector would be weighted much more heavily in IO.3. Likewise, some DNFBPs may be more important than others (e.g. TCSPs in a trust and company formation centre, casinos in a country with a large gaming sector, DPMS in countries with a significant amount of trade in gold or gemstones, etc.) which means that weak supervision or weak preventive measures in that sector would be weighted much more heavily in IO.4 than in countries where such sectors are of lesser importance.

16. For FIs and VASPs under IO.3 and DNFBPs under IO.4, assessors should explain how they have weighted the different sectors, in general terms (e.g. by explaining which sectors were weighted most important, highly important, moderately important or less important) rather than trying to rank each sector's prevalence individually (e.g. 1, 2, 3, 4, 5, 6, 7, 8…) which would be overly granular and a rather artificial distinction given the many different types of financial institutions, VASPs and DNFBPs that are subject to the FATF Recommendations.

1.2.2 Legal persons and legal arrangements

17.

18. Assessors should briefly describe the types of legal persons and legal arrangements that can be established or created in the country and relevant from an AML/CFT perspective.[206] Basic characteristics of these should be provided as well as their numbers registered annually during the review period (to the extent possible) and their significance within the country and in financial and DNFBP sectors. Tables provided by the assessed country in the Chapter 1 questionnaire may be used to summarise the information. The international elements should be covered, particularly the extent to which the country acts as an international centre for the creation or administration of legal persons or arrangements (even if only as a source-of-law jurisdiction); and the extent to which legal persons and arrangements created in another jurisdiction (or under the law of another jurisdiction) hold assets or are used in the country. Assessors should note (based on risk, materiality and context)

205 See Introduction to the *Methodology*, "Sector Materiality and Weighting".

206 See Introduction to the *Methodology*, "Risk and Context".

the relative importance of different types of legal persons and legal arrangements, and their activity.[207] It is important for assessors to explain their weighing of the relative importance of the different types of legal persons and legal arrangements to encourage consistent weighting throughout the MER, particularly when assessing IO.5, R.24 (criterion 24.1)and R.25 (criterion 25.1).

1.3 Structural Elements

19.

20. Assessors should note whether the main structural elements required for an effective AML/CFT system are present in the country including: political stability; a high-level commitment to address AML/CFT/CPF issues; stable institutions with accountability; integrity and transparency; the rule of law; and a capable and efficient judicial system (as set out in paragraph 10 of the introduction to the *Methodology*).

21. If there are serious concerns that any of the structural elements which underpin an effective AML/CFT/CPF system is weak or absent, assessors should highlight those concerns in this section. Note that assessors are not expected to reach a general conclusion about the extent to which such factors are present.

1.4 Background and other Contextual Factors

22.

23. Assessors should note domestic and international contextual factors that might significantly influence the effectiveness of the country's AML/CFT/CPF measures as described in paragraph 11 of the *Methodology*. This could include such factors as: the maturity and sophistication of the AML/CFT/CPF regime and the institutions which implement it; transparency, maturity and sophistication of the criminal justice, regulatory, supervisory and administrative regime in the country; the level of corruption and the impact of measures to combat it; or the level of financial exclusion; exposure to risks from organised crime; or regional instability, including armed conflict, climate related events, natural disasters or irregular migration flows (whether domestic or in neighbouring countries). All other background information necessary for the understanding of the effectiveness analysis in the main chapters of the report should be incorporated here as well. including the following information required by sections 1.4.1 to 1.4.7 below.

1.4.1 AML/CFT/CPF strategy

24.

25. This section should set out the main policies and objectives of the Government for combating money laundering and terrorist financing. It should describe the government's priorities and objectives in these areas, noting where there are also wider policy objectives (such as financial inclusion) which affect the AML/CFT/CPF strategy. Any relevant policies and objectives for combating the financing of proliferation should also be set out in this section.

[207] See the *Methodology*, footnotes to R.24, R.25, and Note to Assessors at Immediate Outcome 3.

1.4.2. Legal & institutional framework

26.

27. Assessors should give a brief overview of which ministries, agencies, and authorities are responsible for formulating and implementing the government's AML/CFT and proliferation financing policies. This includes any relevant authorities at the supra-national or sub-national (i.e., state, province or local) levels (see also paragraphs 28 to 31 of the *Methodology*). Assessors should briefly describe the principal role and responsibilities of each body involved in the AML/CFT strategy, as well as noting the bodies responsible for combating the financing of proliferation. Assessors should indicate any significant changes since the last MER to the institutional framework, including the rationale for those changes. This section should also set out the country's legal framework for AML/CFT/CPF in a brief summary form. Detailed description and analysis of each element is not necessary – this should be included in the technical annex. Assessors should describe the co-operation and coordination mechanisms used by the country to assist the development and implementation of AML/CFT policies, and policies for combating the financing of proliferation.

1.4.3 Preventive measures

28.

29. This section should set out the legal (or other enforceable) instruments through which they are applied, and the scope of such obligations. If assessors identify any problems regarding the scope of AML/CFT obligations, they should briefly identify such issues in this section. If countries have exempted specific sectors or activities from the requirements, these exemptions should be noted in this section. Assessors should indicate whether such exemptions meet the criteria set out in R.1, and whether they consider the exemptions justified based on the country's ML/TF risk assessment(s). This section should also note cases where countries have decided, based on risk, to require AML/CFT preventive measures to be applied by additional sectors which are normally outside the scope of the FATF Recommendations.

1.4.4 Supervisory arrangements[208]

30.

31. Assessors should set out the institutional arrangements for supervision and oversight of financial institutions, VASPs, and DNFBPs, including the roles and responsibilities of regulators, supervisors and SRBs; their general powers and resources. Similarly, this section should also note the institutional framework for legal persons and arrangements, including the authorities (if any) with responsibility for the creation, registration, and supervision of legal persons and arrangements.

1.4.5 International Cooperation

32.

[208] Assessors should describe the supervisory arrangements in place for financial institutions, VASPs, and DNFBPs.

33. Assessors should briefly summarise the international ML/TF risks and threats faced by the country, including the potential use of the country to launder proceeds of crime in other countries and vice-versa. To the extent possible, assessors should identify the country's most significant international partners with respect to ML/TF issues. This section should also note any institutional framework for international cooperation e.g. a Central Authority for MLA.

Table 1.1. <Sample table>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			

Note:
Source:

Box 1.1. <Sample Case Study box (enter title here)>

Note:
Source:

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

2.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Key Recommended Actions (KRA)

a)

b) This section should set out a targeted and prioritised set of recommendations on how the country should improve its level of effectiveness and its level of compliance with the FATF Recommendations. The section should include assessors' recommendations regarding the Immediate Outcomes and Recommendations covered in this chapter of the MER. Assessors will therefore need to consider a range of Outcomes and Recommendations, and actions aimed at addressing both technical deficiencies and practical issues of implementation or effectiveness and decide which actions should be prioritised.

c) Assessors should clearly indicate which Immediate Outcome(s) or Recommendation(s) each recommended action is intended to address. Assessors should follow the same general approach when making recommendations in other chapters of the MER.

d) Key Recommended Actions (KRA) should be noted separately from Other Recommended Actions. If IO.1 is rated HE or SE, delete this section, and reflect all recommended actions for this chapter in the next section on Other Recommended Actions.

e) Key Recommended Actions only relate to Immediate Outcomes rated ME or LE or Recommendations related to PC or NC where these relate to any IO rated ME or LE. There should not normally be more than 2-3 KRAs per Immediate Outcome, including any KRA that concerns a related Recommendation under an Immediate Outcome. Assessors may, in exceptional cases, also set out a limited number of KRAs on contextual factors. In such cases, the KRAs on contextual factors should be linked to an explanation in the MER setting out the grounds for the recommended action and the intended impact on the country's effective compliance with the FATF

Standards.[209]

f) The report should prioritise KRA for remedial measures, taking into account the country's risks and context, its level of effectiveness, and any weaknesses and problems identified. Assessors' recommendations should not simply be to address each of the deficiencies or weaknesses identified but should add value by identifying and prioritising specific and targeted measures in order to most effectively mitigate the risks the country faces, and the deficiencies that exist, and taking into account relevant contextual factors. This could be on the basis that they offer the greatest and most rapid practical improvements, have the widest-reaching effects, or are easiest to achieve.

g) Assessors should be careful to consider the circumstances and context of the country, and its legal and institutional system when making recommendations, noting that there are several different ways to achieve an effective AML/CFT/CPF system, and that their own preferred model may not be appropriate in the context of the country assessed.

h) Assessors should work together with the country to identify the measures needed, so that meaningful recommendations can be made. It is important that the recommendations, and particularly the KRAs, are drafted in a way that is practical, achievable and precise and clear, without being overly prescriptive. They also should be measurable and time-bound, so that the progress achieved can be benchmarked, and be outcome oriented and targeted, so that they result in increased effectiveness.

i) To facilitate the development of an action plan by the assessed country, assessors should clearly indicate in their recommendations where a specific action is required, and where there may be some flexibility about how a given priority objective is to be achieved. Assessors should avoid making unnecessarily rigid or overly detailed recommendations (e.g., on the scheduling of certain measures or the prosecution of specific persons), so as not to hinder countries efforts to fully adapt the recommendations to fit local circumstances.

Other Recommended Actions

a)

b) If IO.1 is rated HE or SE, all recommended actions for this chapter should appear in this section.

c) Even if a country has a high level of effectiveness, this does not imply that there is no further room for improvement. There may also be a need for action in order to sustain a high level of effectiveness in the face of evolving risks. If assessors are able to identify further actions in areas where there is a high degree of effectiveness, then they should also include these in their recommendations.

d) Ordinarily, there should be no more than five recommended actions per Immediate Outcome.

[209] See *Methodology*, Introduction para. 64 for guidance.

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

2.2 Immediate Outcome 1 (Risk, Policy and Coordination)

35. This section should set out assessors' analysis of Immediate Outcome 1. The first paragraph(s) should note any general considerations regarding the country's risks and context which affect the assessment.

36. This section should also summarise assessors' general impression of whether the country appears to exhibit the characteristics of an effective system.

37. Assessors should cover each of the Core Issues in their analysis. Assessors have some flexibility about how they organise the analysis in this section. For some immediate outcomes, it may be appropriate to consider each of the core issues in turn. For others (e.g. IO.3 and IO.4) it may be better to set out the analysis sector-by-sector; or (e.g. for I.O.7) to proceed step-by-step with the analysis of each element of the process covered by the Outcome. Whichever approach assessors take to organising their analysis, they should ensure that they consider each of the core issues and ***should highlight any general conclusions they reach on them***. Assessors should use sub-headings to structure their analysis and clearly sign-post how core issues have been addressed. This does not preclude the use of additional sub-headings where necessary or to indicate that a particular Core Issue is not applicable in a particular country (and why). In the case of IO.1, this includes the suggested sub-headings below.

38. Examples of sub-headings for other IOs are provided in this template. Assessors still retain full flexibility to amend and order these as most benefit their analysis and the overall report. Similarly, assessors may add or delete sub-headings as they see fit and in line with the specific circumstances of the assessed country. In all cases sub-headings should be neutral and not provide any qualitative comment as to how the country is performing on a given IO. Assessors should note the main sources of information and evidence used (e.g. the sources noted in sections (a) and (b) of the Immediate Outcome). Assessors are not required to use all the information noted in the *Methodology* – but should set out here the information and evidence which has a material influence on their conclusion. Assessors should also note in their analysis any technical compliance issues which influence the level of effectiveness.

39. Some of the factors assessed under Immediate Outcome 1 that consider the country's assessment of risks and implementation of the risk-based approach may have far-reaching effects on other outcomes (e.g., risk assessment affects the application of risk-based measures under Immediate Outcomes 3 and 4, and the deployment of competent authorities' resources relative to all outcomes). However, where possible, assessors should avoid duplication. Assessors should present their analysis of a particular issue once, in what they consider is the most relevant section of the MER, then cross-reference this analysis in other parts of the MER where the issue is relevant. See the Introduction to the *Methodology* section on Cross-cutting Issues.

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

ML risks

40.

TF Risks

41.

2.2.2 National policies and activities to address identified ML/TF risks

Policies and activities to address ML risks

42.

Policies and activities to address TF Risks

43.

2.2.3 Exemptions, enhanced and simplified ML/TF measures

ML measures

44.

TF measures

45.

2.2.4 Objectives and activities of competent authorities and SRBs

46.

2.2.5 National coordination and cooperation to develop and implement policy

47.

2.2.6 National coordination and cooperation for operational purposes

48.

Overall Conclusion on IO.1

49. [Weighting and conclusion]

50. [Evaluated country] is rated as having a [rating] level of effectiveness for IO.1.

51. At the end of this section, assessor***s should indicate the effectiveness rating for the Immediate Outcome***. When deciding on the overall level of effectiveness, assessors should take into account: (a) the core issues, (b) any relevant technical compliance issues/deficiencies that are significantly impacting effectiveness; (c) risks and contextual factors; and (d) the level of effectiveness in other Immediate Outcomes that are relevant and are significantly impacting effectiveness in this area. Assessors should briefly explain their conclusion on the appropriate effectiveness rating. They should be explicit about the weight and importance they attach to the elements taken into account. The conclusion should not duplicate the Key Findings section at the beginning of each chapter and should be, ideally, not more than one or two paragraphs long.

52. Assessors should follow the same general approach when setting out their analysis of effectiveness for all other Immediate Outcomes.

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary or remove.

Table 2.1. <Sample table>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			

Note:
Source:

Box 2.1. <Sample Case Study box (enter title here)>

Note:
Source:

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

3.1 Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Key Recommended Actions (KRA)

a)

a) Assessors should list all the main corrective actions required for the country to improve its level of effectiveness and technical compliance in a targeted and prioritised way. Assessors should clearly indicate which IO/REC the recommended actions relate to.

b) Key Recommended Actions (KRA) should be noted separately from Other Recommended Actions. Key Recommended Actions only relate to Immediate Outcomes rated ME or LE or Recommendations related to PC or NC where these relate to any IO rated ME or LE. If IO.6, IO.7 and IO.8 are all rated HE or SE, and R.3 is rated LC or C, delete this section, and reflect all recommended actions for this chapter in the next section on Other Recommended Actions.

c) There should not normally be more than 2-3 KRAs per Immediate Outcome, including KRA for technical compliance for Recommendations related to that IO. In addition, there may be one KRA for R.3 that is rated NC or PC, regardless of the rating for IO.7.

Other Recommended Actions

a) If IO.6, IO.7 and IO.8 are all rated HE or SE, and R.3 is rated LC or C, all recommended actions for this chapter should appear in this section.

b) Ordinarily, there should be no more than five recommended actions per Immediate Outcome.

53. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 34, 37, 38, 39 and 40.

3.2 Immediate Outcome 6 (Financial Intelligence ML/TF)

54. This Immediate Outcome relates to both money laundering and the financing of terrorism. Assessors should note any issues which relate specifically to either ML or TF. Sub-headings related to core issues could include:

3.2.1. Timely access to relevant, accurate and up-to-date information

By the FIU

55.

By other competent authorities

56.

3.2.2. Production and dissemination of financial intelligence

Production of financial intelligence

Dissemination of financial intelligence

FIU financial intelligence supporting needs of competent authorities

57.

Other competent authorities producing financial intelligence (where relevant)

58.

3.2.3. Cooperation and exchange of information/financial intelligence

Co-operation and exchange

59.

Security and confidentiality

60.

3.2.4. Using information/financial intelligence

Using information / financial intelligence for investigations and developing evidence

61.

Using information / financial intelligence to assist in identifying and tracing criminal proceeds or instrumentalities

62.

Overall conclusion on IO.6

63. [Weighting and conclusion: See IO.1 for instructions]

64. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.6.**

3.3 Immediate Outcome 7 (ML investigation and prosecution)

3.3.1. ML activity identified and investigated

65.

3.3.2. Prosecuting and convicting different types of ML activity[210]

66.

3.3.3. Effectiveness, proportionality and dissuasiveness of sanctions

67.

3.3.4. Use of alternative measures

68.

Overall conclusion on IO.7

69. [Weighting and conclusion: See IO.1 for instructions]

70. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.7.**

3.4 Immediate Outcome 8 (Confiscation)

3.4.1. Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

71.

[210] See *Methodology*, IO.7, Note to Assessors 2 and related footnotes.

3.4.2. Confiscation of proceeds, instrumentalities and property of equivalent value from foreign and domestic predicates, and proceeds located abroad

Confiscation – domestic and foreign predicate offences

72.

Confiscation – proceeds located abroad

73.

Repatriation, sharing and restitution

74.

3.4.3. Confiscation of falsely or undeclared cross-border transaction of currency/BNI

75.

3.4.4. Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

76.

Overall conclusion on IO.8

77. [Weighting and conclusion: See IO.1 for instructions]
78. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.8.**

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary or remove.

Table 3.1. <Sample table>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			

Note:
Source:

Box 3.1. <Sample Case Study box (enter title here)>

Note:
Source:

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

4.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Key Recommended Actions (KRA)

a)

b) Assessors should briefly list the main corrective actions required for the country to improve its level of effectiveness and technical compliance. Assessors should clearly indicate which IO/REC the recommended actions relate to.

c) Key Recommended Actions (KRA) should be noted separately from Other Recommended Actions. Key Recommended Actions only relate to Immediate Outcomes rated ME or LE or Recommendations related to PC or NC where these relate to any IO rated ME or LE. If IO.9, IO.10 and IO.11 are all rated HE or SE, and R.5 and R.6 are both rated LC or C, delete this section, and reflect all recommended actions for this chapter in the next section on Other Recommended Actions.

d) There should not normally be more than 2-3 KRAs per Immediate Outcome, including KRA for technical compliance for Recommendations related to that IO. In addition, there may be one KRA for R.5 that is rated NC or PC, regardless of the rating for IO.9, and one KRA for R.6 that is rated NC or PC, regardless of the rating for IO.10.

Other Recommended Actions

a) If IO.9, IO.10 and IO.11 are all rated HE or SE, and R.5 and R.6 are both rated LC or C, all recommended actions for this chapter should appear in this section.

b) Ordinarily, there should be no more than five recommended actions per Immediate Outcome.

79. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

4.2. Immediate Outcome 9 (TF investigation and prosecution)

4.2.1. TF activity identified and investigated

Identification and investigation of TF activity

80.

Investigations identifying the specific role of terrorist financier

81.

4.2.2. Prosecuting and convicting different types of TF

82.

4.2.3. Effectiveness, proportionality and dissuasiveness of sanctions

83.

4.2.4. National counter-terrorism strategies and activities

Formulating national counter-terrorism strategies and activities

84.

Sharing and using information and intelligence to support national counter-terrorism purposes and activities

85.

4.2.5. Alternative measures used where TF conviction is not possible (e.g. disruption)

86.

Overall conclusions on IO.9

87. [Weighting and conclusion: See IO.1 for instructions]
88. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.9.**

4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)

4.3.1. Implementation of TF-related targeted financial sanctions without delay

89.

4.3.2. Identification and deprivation of terrorist funds or other assets

90.

4.3.3. Targeted application of focused and proportionate mitigation measures to at-risk non-profit organisations

91.

4.3.4. FIs, VASPs and DNFBPs understanding of and compliance with obligations

FIs and VASPs

92.

DNFBPs

93.

4.3.5. Competent authorities monitoring and ensuring compliance with TF-related targeted financial sanctions

FIs and VASPs

94.

DNFBPs

95.

Overall conclusions on IO.10

96. [Weighting and conclusion: See IO.1 for instructions]
97. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.10**.

4.4. Immediate Outcome 11 (PF financial sanctions)

4.4.1. Competent authorities co-operation and co-ordination to combat PF financing

Co-operation and co-ordination to develop and implement policy

98.

Co-operation and, where appropriate, co-ordination for operational purposes

99.

4.4.2.Understanding and mitigating the risk of breach, non-implementation or evasion of PF-related targeted financial sanctions

100.

4.4.3. Implementation of PF-related targeted financial sanctions without delay

101.

4.4.4. Identification of assets and funds held by designated persons/entities/those acting on their behalf and prohibitions

Identifying funds or assets held by designated persons/entities/persons acting on their behalf or at their direction

102.

Prohibiting financial transactions related to proliferation

103.

4.4.3. FIs, VASPs and DNFBPs understanding of and compliance with obligations

FIs and VASPs

104.

DNFBPs

105.

4.4.4. Competent authorities monitoring and ensuring compliance with PF-related targeted financial sanctions

FIs and VASPs

106.

DNFBPs

107.

Overall conclusion on IO.11

108. [Weighting and conclusion: See IO.1 for instructions]

109. [Evaluated country] is rated as having a [rating] level of effectiveness for IO.11.

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary or remove.

Table 4.1. <Sample table>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			

Note:
Source:

Box 4.1. <Sample Case Study box (enter title here)>

Note:
Source:

CHAPTER 5. SUPERVISION AND PREVENTIVE MEASURES

5.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Key Recommended Actions (KRA)

a)

b) Assessors should briefly list the main corrective actions required for the country to improve its level of effectiveness and technical compliance. Assessors should clearly indicate which IO/REC the recommended actions relate to.

c) Key Recommended Actions (KRA) should be noted separately from Other Recommended Actions. Key Recommended Actions only relate to Immediate Outcomes rated ME or LE or Recommendations related to PC or NC where these relate to any IO rated ME or LE. If IO.3 and IO.4, are both rated HE or SE, and R.10, 11 and 20 are all rated LC or C, delete this section, and reflect all recommended actions for this chapter in the next section on Other Recommended Actions.

d) There should not normally be more than 2-3 KRAs per Immediate Outcome, including KRA for technical compliance for Recommendations related to that IO. In addition, there may be one KRA for each of R.10, R.11 and R.20 that is rated NC or PC, regardless of the rating for IO.3.

Other Recommended Actions

a) If IO.3 and IO.4 are both rated HE or SE, and R.10, 11 and 20 are all rated LC or C, all recommended actions for this chapter should appear in this section.

b) Ordinarily, there should be no more than five recommended actions per Immediate Outcome. If IO.3 and IO.4 are both rated HE or SE, and R.10, 11 and 20 are all rated LC or C, all recommended actions for this chapter should appear in this section.

110. The relevant Immediate Outcomes considered and assessed in this chapter are IO.3 and IO.4.[211] The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, 26, 27, 28, 34 and 35, and elements of R.1, 29 and 40.

5.2. Immediate Outcome 3 (Supervision and Preventive Measures for Financial Institutions (FIs) and VASPs)

Notes for Assessors:

The first paragraph should give a short summary of what relative importance assessors have given to the different types of financial institutions and VASPs, taking into account the risk, context and materiality of the country being assessed. This should be supplemented by a cross-reference to the more detailed information in Chapter One on how each sector has been weighted (based on risk, context and materiality) (as required in the instructions under that heading in the *Methodology*).

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

Market entry controls

111.

Detecting and addressing breaches

112.

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

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

113.

[211] When assessing effectiveness under Immediate Outcomes 3 and 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 Financial Institutions, DNFBPs and VASPs, as required in the instructions under that heading in the *Methodology*.

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

114.

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

115.

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

CDD, record-keeping, BO information, ongoing monitoring

116.

Enhanced or specific measures

117.

AML/CFT reporting obligations, tipping off

118.

Internal controls, procedures and audit to ensure compliance

119.

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

120.

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

121.

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

122.

Overall conclusion on IO.3

123. [Weighting and conclusion]

124. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.3.**

5.3. Immediate Outcome 4 (Supervision and Preventive Measures for DNFBPs)

Notes for Assessors:

The first paragraph should give a short summary of what relative importance assessors have given to the different types of DNFBPs, taking into account the risk, context and materiality of the country being assessed. This should be supplemented by a cross-reference to the more detailed information in Chapter One on how each sector has been weighted (based on risk, context and materiality) (as required in the instructions under that heading in the *Methodology*).

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

Market entry controls

125.

Detecting and addressing breaches

126.

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

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

127.

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

128.

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

129.

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

CDD, record-keeping, BO information, ongoing monitoring

130.

Enhanced or specific measures

131.

AML/CFT reporting obligations, tipping off

132.

Internal controls, procedures and audit to ensure compliance

133.

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

134.

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

135.

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

136.

Overall conclusions on IO.4

137. [Weighting and conclusion]

138. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.4.**

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary or remove.

Table 5.1. <Sample table>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			

Note:
Source:

Box 5.1. <Sample Case Study box (enter title here)>

Note:
Source:

CHAPTER 6. LEGAL PERSONS AND ARRANGEMENTS

6.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Key Recommended Actions (KRA)

a)

b) Assessors should briefly list the main corrective actions required for the country to improve its level of effectiveness and technical compliance. Assessors should clearly indicate which IO/REC the recommended actions relate to.

c) Key Recommended Actions (KRA) should be noted separately from Other Recommended Actions. Key Recommended Actions only relate to Immediate Outcomes rated ME or LE or Recommendations related to PC or NC where these relate to any IO rated ME or LE. If IO.5 is rated HE or SE, delete this section, and reflect all recommended actions for this chapter in the next section on Other Recommended Actions.

d) There should not normally be more than 2-3 KRAs per Immediate Outcome, including KRA for technical compliance for Recommendations related to that IO.

139. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37 and 40.[212]

6.2. Immediate Outcome 5 (Legal Persons and Arrangements)

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

140.

[212] 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.

6.2.2. Mitigating measures preventing misuse of legal persons and arrangements

141.

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

142.

6.2.4. Legal arrangements: Timely access to adequate, accurate and current basic and beneficial ownership information[213]

143.

6.2.5. Effectiveness, proportionality and dissuasiveness of sanctions

144.

Overall conclusion on IO.5

145. [Weighting and conclusion: See IO.1 for instructions]

146. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.5.**

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary, or remove.

213 See the *Methodology* for Recommendation 25 regarding beneficial ownership information for legal arrangements.

Table 6.1. <Sample table>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			

Note:
Source:

Box 6.1. <Sample Case Study box (enter title here)>

Note:
Source:

CHAPTER 7. INTERNATIONAL COOPERATION

7.1. Key Findings and Recommended Actions

Key Findings

a)

b) Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings. Key findings and key recommended actions should be consistent on the substance without a need to strictly mirror each other.

Key Recommended Actions (KRA)

a)

b) Assessors should briefly list the main corrective actions required for the country to improve its level of effectiveness and technical compliance. Assessors should clearly indicate which IO/REC the recommended actions relate to.

c) Key Recommended Actions (KRA) should be noted separately from Other Recommended Actions. Key Recommended Actions only relate to Immediate Outcomes rated ME or LE or Recommendations related to PC or NC where these relate to any IO rated ME or LE. If IO.2 is rated HE or SE, delete this section, and reflect all recommended actions for this chapter in the next section on Other Recommended Actions.

d) There should not normally be more than 2-3 KRAs per Immediate Outcome, including KRA for technical compliance for Recommendations related to that IO.

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

7.2. Immediate Outcome 2 (International Co-operation)

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

Providing evidence and locating criminals

148.

Extradition

149.

Identifying, freezing, seizing, confiscating and sharing criminal assets

150.

7.2.2. Seeking appropriate and timely mutual legal assistance and extradition

Seeking evidence and locating criminals

151.

Extradition

152.

Seeking to identify, freeze, seize, confiscate and share criminal assets

153.

7.2.3. Seeking other forms of international cooperation for AML/CFT purposes, including asset recovery

FIU

154.

Law enforcement agencies (LEAs)

155.

Supervisors of FIs, VASPs and DNFBPs

156.

Customs and tax authorities

157.

7.2.4. Providing other forms international cooperation for AML/CFT purposes, including asset recovery

FIU

158.

Law enforcement agencies (LEAs)

159.

Supervisors of FIs, VASPs and DNFBPs

160.

Customs and tax authorities

161.

162.

Overall conclusions on IO.2

163. [Weighting and conclusion: See IO.1 for instructions]

164. **[Evaluated country] is rated as having a [rating] level of effectiveness for IO.2.**

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary or remove.

Table 7.2. <Sample table>

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			

Note:
Source:

Box 7.2. <Sample Case Study box (enter title here)>

Note:
Source:

ANNEX A. TECHNICAL COMPLIANCE ANNEX

1. 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.
2. This technical compliance covers only Recommendations where the country has made legal, regulatory or operational framework changes since its last mutual evaluation (dated [XX]) (or follow-up reports with technical compliance re-ratings (dated [XX], and [XX])[214] and Recommendations where there has been a change in the FATF Standards for which the country has not previously been assessed. The latter Recommendations are identified with the Recommendation heading in green text.
3. For Recommendations not under review, pre-existing information from the country's most recent assessments has been compiled for inclusion in this annex. 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).
4.

1. Recommendation 1 – Assessing risks and applying a risk-based approach

For each Recommendation, an opening paragraph should set out:

- the rating given in the previous MER, where applicable, and the main deficiencies identified;
- any conclusions reached in the follow-up process about whether the country has addressed its deficiencies;
- indication that there are new FATF requirements against which the country has not yet been assessed, relative to the *2013 Methodology*; and
- the main changes to the relevant laws, regulations, and other elements in the country since the country was last assessed.

All countries should be evaluated on the basis of the FATF Standards and *Methodology* as they exist at the date the country's technical compliance submission is due. For any FATF Recommendation revised within the 24 months prior to a country's onsite visit, the opening paragraph should contain a footnote clearly stating that this aspect of the assessment has been made against recently amended Standards.

Criterion 1.1 – (Met / Mostly met / Partly met / Not met)

Each of the criteria should be reviewed, normally in a single paragraph.

[214] For details regarding how these Recommendations are identified, please refer to the section on Technical Compliance Review in your assessment body's Procedures or the *Universal Procedures.*

If one or more criteria have been considered previously and the relevant laws, enforceable means, or other elements are unchanged, assessors should not repeat the previous analysis. Instead, they should summarise the conclusions, and include a reference to the report where the detailed analysis is set out (including paragraph numbers where feasible). Such references should only be made to MERs, FSAPs, or FUR with TCRR which are publicly available; were analysed, considered, and adopted by an assessment body; and if assessors consider the analysis and conclusion were correct.

For each criterion, and prior to the narrative, the assessment team should set out in parenthesis whether the country is meeting FATF requirements. These sub-ratings will ultimately be removed before publication but will guide discussions ahead of and during the Plenary.

Criterion 1.2 – (Met / Mostly met / Partly met / Not met)

Assessors should include only their analysis of whether the criterion is met. General descriptions of the country's situation, context, or of the legal and institutional framework should be included in the main report, and not in this annex (though assessors may cross-reference any relevant points in the main report).

Assessors have flexibility to devote more space to their analysis where necessary, particularly to complex criteria or criteria which apply to a number of different sectors. In such cases, it may be helpful to set out their analysis in the form of a table. However, assessors should remember that the overall length of this technical annex should normally be limited to a maximum of 60 pages.

Weighting and Conclusion

Assessors should set out their conclusion on the appropriate technical compliance rating, and the reasoning for this. They should be explicit about the importance they attach to each of the criteria that particularly impact the rating (including with reference to the country's risk and context, as set out in the main MER). **The rating should be stated in bold at the end of the paragraph.**

2. Recommendation 2 - National Cooperation and Coordination

Criterion 2.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

3. Recommendation 3 - Money laundering offence

Criterion 3.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

4. Recommendation 4 - Confiscation and provisional measures

Criterion 4.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

5. Recommendation 5 - Terrorist financing offence

Criterion 5.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

6. Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

Criterion 6.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

7. Recommendation 7 – Targeted financial sanctions related to proliferation

Criterion 7.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

8. Recommendation 8 – Non-profit organisations

Criterion 8.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

9. Recommendation 9 – Financial institution secrecy laws

Criterion 9.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

10. Recommendation 10 – Customer due diligence

Criterion 10.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

11. Recommendation 11 – Record-keeping

Criterion 11.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

12. Recommendation 12 – Politically exposed persons

Criterion 12.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

13. Recommendation 13 – Correspondent banking

Criterion 13.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

14. Recommendation 14 – Money or value transfer services

Criterion 14.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

15.Recommendation 15 – New technologies

Criterion 15.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

16.Recommendation 16 – Wire transfers

Criterion 16.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

17.Recommendation 17 – Reliance on third parties

Criterion 17.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

18.Recommendation 18 – Internal controls and foreign branches and subsidiaries

Criterion 18.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

19.Recommendation 19 – Higher-risk countries

Criterion 19.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

20.Recommendation 20 – Reporting of suspicious transaction

Criterion 20.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

21.Recommendation 21 – Tipping-off and confidentiality

Criterion 21.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

22.Recommendation 22 – DNFBPs: Customer due diligence

Criterion 22.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

23.Recommendation 23 – DNFBPs: Other measures

Criterion 23.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

24.Recommendation 24 – Transparency and beneficial ownership of legal persons

Criterion 24.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

25.Recommendation 25 – Transparency and beneficial ownership of legal arrangements

Criterion 25.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

26.Recommendation 26 – Regulation and supervision of financial institutions

Criterion 26.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

27.Recommendation 27 – Powers of supervisors

Criterion 27.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

28.Recommendation 28 – Regulation and supervision of DNFBPs

Criterion 28.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

29.Recommendation 29 - Financial intelligence units

Criterion 29.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

30.Recommendation 30 – Responsibilities of law enforcement and investigative authorities

Criterion 30.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

31.Recommendation 31 - Powers of law enforcement and investigative authorities

Criterion 31.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

32.Recommendation 32 – Cash Couriers

Criterion 32.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

33.Recommendation 33 – Statistics

Criterion 33.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

34.Recommendation 34 – Guidance and feedback

Criterion 34.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

35.Recommendation 35 – Sanctions

Criterion 35.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

36.Recommendation 36 – International instruments[215]

Criterion 36.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

37.Recommendation 37 - Mutual legal assistance

Criterion 37.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

215 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.

38.Recommendation 38 – Mutual legal assistance: freezing and confiscation

Criterion 38.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

39.Recommendation 39 – Extradition

Criterion 39.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

40.Recommendation 40 – Other forms of international cooperation

Criterion 40.1 – (Met / Mostly met / Partly met / Not met)

Weighting and Conclusion

The following are templates for tables and case studies for use in this section Chapter. Copy and paste where necessary or remove.

Annex Table 1.

	Note to assessors: please ensure that tables and boxes are numbered per Chapter			

Note:
Source:

Annex Box 1. <Sample Case Study box (enter title here)>

Note:
Source:

TECHNICAL COMPLIANCE DEFICIENCIES

Annex Table 2. Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	[C]	This table should set out the rating, and a list of all deficiencies identified for each Recommendation.
2. National cooperation and coordination	[LC]	•
3. Money laundering offences	[PC]	•
4. Confiscation and provisional measures	[NC]	•
5. Terrorist financing offence		•
6. Targeted financial sanctions related to terrorism & TF		•
7. Targeted financial sanctions related to proliferation		•
8. Non-profit organisations		•
9. Financial institution secrecy laws		•
10. Customer due diligence		•
11. Record keeping		•
12. Politically exposed persons		•
13. Correspondent banking		•
14. Money or value transfer services		•
15. New technologies		•
16. Wire transfers		•
17. Reliance on third parties		•
18. Internal controls and foreign branches and subsidiaries		•

Recommendations	Rating	Factor(s) underlying the rating
19. Higher-risk countries		•
20. Reporting of suspicious transaction		•
21. Tipping-off and confidentiality		•
22. DNFBPs: Customer due diligence		•
23. DNFBPs: Other measures		•
24. Transparency and beneficial ownership of legal persons		•
25. Transparency and beneficial ownership of legal arrangements		•
26. Regulation and supervision of financial institutions		•
27. Powers of supervisors		•
28. Regulation and supervision of DNFBPs		•
29. Financial intelligence units		•
30. Responsibilities of law enforcement and investigative authorities		•
31. Powers of law enforcement and investigative authorities		•
32. Cash couriers		•
33. Statistics		•
34. Guidance and feedback		•
35. Sanctions		•
36. International instruments		•
37. Mutual legal assistance		•
38. Mutual legal assistance: freezing and confiscation		•

Recommendations	Rating	Factor(s) underlying the rating
39. Extradition		•
40. Other forms of international cooperation		•

Note:

GLOSSARY OF ACRONYMS[216]

	DEFINITION
AML/CFT/CPF	Anti-Money Laundering, Combating the Financing of Terrorism and Combatting the Financing of Proliferation of Weapons of Mass Destruction

Note:
Source:

216 Acronyms already defined in the *FATF 40 Recommendations* are not included into this Glossary.

ANNEX II: FATF GUIDANCE DOCUMENTS

Assessors may consider FATF Guidance as background information on the practicalities of how countries can implement specific requirements. However, assessors should remember that FATF guidance is ***non-binding***. The application of any guidance should not form part of the assessment. See Methodology paragraph 37.

Guidance	Relevant FATF Standards/Methodology
National money laundering and terrorist financing risk assessment (Mar 2013) Terrorist Financing Risk Assessment Guidance (Jul 2019) Guidance on Proliferation Financing Risk Assessment and Mitigation (Jun 2021)	**R.1** (Assessing Risks and Applying a Risk Based Approach)
Best Practices Paper on Recommendation 2: Sharing among domestic competent authorities information related to the financing of proliferation (Mar 2012)	**R.2** (National Co-operation and Co-ordination) **R.7** (TFS Related to Proliferation)
Best Practices on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery (Oct 2012)	**R.4** (Confiscation and Provisional Measures) **R.38** (Freezing and Confiscation)
Guidance on Criminalising Terrorist Financing (Oct 2016)	**R.5** (Terrorist Financing Offence)
International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6) (Jun 2013)	**R.6** (Targeted Financial Sanctions related to Terrorism and Terrorist Financing)
FATF Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction (Feb 2018)	**R.7** (Targeted Financial Sanctions related to Proliferation)
Best Practices on Combating the Abuse of Non-Profit Organisations Profit Organisations (Nov 2023)	**R.8** (Non-Profit Organisations (NPOs)
Guidance on Digital ID (Mar 2020)	**R.10** (Customer due diligence (CDD)=
FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22) (Jun 2013)	**R.12** (Politically Exposed Persons (PEPs)) **R.22** (Designated Non-Financial Businesses and

Guidance	Relevant FATF Standards/Methodology
	Professions (DNFBPs): Customer Due Diligence)
Guidance on Correspondent Banking Services (Oct 2016)	**R.13** (Correspondent Banking)
Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Oct 2021)	**R.15** (New technologies)
FATF Guidance - Private Sector Information Sharing (Nov 2017)	**R.18** (Internal Controls and Foreign Branches and Subsidiaries) **R.21** (Tipping-Off and Confidentiality)
Guidance on Transparency and Beneficial Ownership (Oct 2014) Beneficial Ownership of Legal Persons (Mar 2023)	**R.24** (Transparency and Beneficial Ownership of Legal Persons) **R.25** (Transparency and Beneficial Ownership of Legal Arrangements) **Methodology IO.5** (Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments)
Guidance on risk based supervision (Mar 2021)	**R.26** (supervision of financial institutions)
Operational Issues - Financial Investigations Guidance (Jul 2012)	**R.30** (Responsibilities of Law Enforcement and Investigative Authorities) **R.31** (Powers of Law Enforcement and Investigative Authorities) **Methodology IO.7** (Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions)
Guidance on AML/CFT-related data and statistics (Nov 2015)	**R.33** (Statistics) **Methodology** *Effectiveness Assessment*
Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement (Oct 2015)	**Methodology IO.3** (Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks)
FATF Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence (Nov 2017)	**Methodology IO.4** (Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions)
Best Practices Paper: The Use of the FATF	**Methodology** *Introduction* (Corruption)

This document is shared for information only. The Methodology in this document will apply to the 5th Round of Mutual Evaluations. It is not yet in effect and may be subject to change before the start of the 5th Round.

Guidance		Relevant FATF Standards/Methodology
Recommendations to Combat Corruption (Oct 2013)		
▯	Guidance for a Risk Based Approach for Legal Professionals (Jun 2019)	**Methodology** *Introduction* (RBA)
▯	Guidance for a Risk-Based Approach for the Accounting Profession (Jun 2019)	
▯	Guidance for a Risk-Based Approach for Trust and Company Service Providers (Jun 2019)	
▯	Guidance for a Risk-Based Approach: Life Insurance Sector (Oct 2018)	
▯	Guidance for a Risk-Based Approach: Securities Sector (Oct 2018)	
▯	Guidance for a Risk-Based Approach: Money or Value Transfer Services (Feb 2016)	
▯	Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement (Oct 2015)	
▯	Guidance for a Risk-Based Approach: Virtual Currencies (Jun 2015)	
▯	Guidance for a Risk-Based Approach: The Banking Sector (Oct 2014)	
	Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services (June 2013)	
	Risk Based Approach Guidance for the Real Estate Sector (July 2022)	

ANNEX III: INFORMATION ON UPDATES MADE TO THE FATF METHODOLOGY

[The following amendments have been made to the FATF Methodology since the text was adopted in February 2022.]

Date	Type of amendments		Sections subject to amendments
June 2023	Revisions to ensure that mutual evaluations consider unintended consequences of the implementation of the FATF Standards.		Introduction paragraphs 7, 10, 22 and 73 (pages 7-9; 12, 26).
June 2023	Addition of footnote to criterion 36.2 to clarify the distinction between FATF and UNODC IRM assessments.		R.36 (criterion 36.2) – page 95
October 2023	Revised the criteria for R.24 and R.25, and revised IO.5 to reflect revisions in the FATF Standards on beneficial ownership. Added cross-references to the Glossary throughout the Methodology to give better guidance to assessors. Added an additional example of information that could support the conclusions on Core Issues for IO.3 and IO.4.		R.24, R.25 and Immediate Outcome 5. Added a new Note to Assessors at the start of each Recommendation and Immediate Outcome cross-referencing the relevant Glossary definitions. Immediate Outcome 3 – Added new paragraph 6 to the *Examples of Information that could support the conclusions on Core Issues.* Immediate Outcome 4 – Added new paragraph 7 to the *Examples of Information that could support the conclusions on Core Issues.*
February 2024	Revision of R.8 and IO.10 to clarify requirements under the FATF Standards regarding Non-profit Organisations (NPOs) Revision of R.23 to clarify that criterion 23.2 applies to DNFBPs		R.8 (*Note to Assessors*, criteria 8.1, 8.2 (b) – (d), 8.3, 8.4(a), 8.5(c) Immediate Outcome 10 – *Characteristics of an effective System*; *Note to assessors* paragraph 1; Core Issue 10.3; New paragraphs 10 and 11 and amended paragraphs 12 – 14 and 17 of *Examples of Information that could support the conclusions on Core Issues.* *Note to Assessors*