FATF

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI-MONEY LAUNDERING MEASURES AND THE FINANCING OF TERRORISM (MONEYVAL)

THE FATF RECOMMENDATIONS

INTERNATIONAL STANDARDS
ON COMBATING MONEY LAUNDERING
AND THE FINANCING OF TERRORISM
& PROLIFERATION

METHODOLOGY

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

RULES OF PROCEDURE

FOR THE 5TH ROUND OF MUTUAL EVALUATIONS
BY MONEYVAL

THE FATF RECOMMENDATIONS
INTERNATIONAL STANDARTS ON COMBATING MONEY LAUNDERING
AND THE FINANCING OF TERRORISM & PROLIFERATION[1]

METHODOLOGY
FOR ASSESING TECHNICAL COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS[2]

RULES OF PROCEDURE
FOR THE 5TH ROUND OF MUTUAL EVALUATIONS[3]
BY MONEYVAL

November 2023

[1] According to the FATF Plenary decision from November 2023.
[2] According to the FATF Plenary decision from June 2023.
[3] Adopted by MONEYVAl at its 46th Plenary meeting (Strasbourg, 8-12 December 2014), last revised through written procedure in the 4th Intersessisonal Consultation (Strasbourg, October 2021).

Contents

THE FATF RECOMMENDATIONS

No.	Old No.	Title
		A - AML/CFT POLICIES AND COORDINATION
1	-	Assessing risks & applying a risk-based approach*
2	R.31	National cooperation and coordination
		B - MONEY LAUNDERING AND CONFISCATION
3	R.1 & R.2	Money laundering offence*
4	R.3	Confiscation and provisional measures*
		C - TERRORIST FINANCING AND FINANCING OF PROLIFERATION
5	SRII	Terrorist financing offence*
6	SRIII	Targeted financial sanctions related to terrorism & terrorist financing*
7		Targeted financial sanctions related to proliferation*
8	SRVIII	Non-profit organisations*
		D - PREVENTIVE MEASURES
9	R.4	Financial institution secrecy laws
		Customer due diligence and record keeping
10	R.5	Customer due diligence*
11	R.10	Record keeping
		Additional measures for specific customers and activities
12	R.6	Politically exposed persons*
13	R.7	Correspondent banking*
14	SRVI	Money or value transfer services*
15	R.8	New technologies
16	SRVII	Wire transfers*
		Reliance, Controls and Financial Groups
17	R.9	Reliance on third parties*
18	R.15 & R.22	Internal controls and foreign branches and subsidiaries*
19	R.21	Higher-risk countries*
		Reporting of suspicious transactions
20	R.13 & SRIV	Reporting of suspicious transactions*
21	R.14	Tipping-off and confidentiality
		Designated non-financial Businesses and Professions (DNFBPs)
22	R.12	DNFBPs: Customer due diligence*
23	R.16	DNFBPs: Other measures *
		E - TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
24	R.33	Transparency and beneficial ownership of legal persons *
25	R.34	Transparency and beneficial ownership of legal arrangements *
		F - POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
		Regulation and Supervision

No.	Old No.	Title
26	R.23	Regulation and supervision of financial institutions*
27	R.29	Powers of supervisors
28	R.24	Regulation and supervision of DNFBPs
		Operational and Law Enforcement
29	R.26	Financial intelligence units*
30	R.27	Responsibilities of law enforcement and investigative authorities*
31	R.28	Powers of law enforcement and investigative authorities
32	SRIX	Cash couriers*
		General Requirements
33	R.32	Statistics
34	R 25	Guidance and feedback
		Sanctions
35	R.17	Sanctions
		G - INTERNATIONAL COOPERATION
36	R.35 & SRI	International instruments
37	R.36 & SRV	Mutual legal assistance
38	R.38	Mutual legal assistance: freezing and confiscation*
39	R.39	Extradition
40	R.40	Other forms of international cooperation*

1. The "Old No." column refers to the corresponding 2003 FATF Recommendation. * Recommendations marked with an asterisk have interpretive notes, which should be read in conjunction with the Recommendation.

   Version as adopted on 15 February 2012.

INTRODUCTION TO THE FATF RECOMMENDATIONS

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Recommendations set out the essential measures that countries should have in place to:

- identify the risks, and develop policies and domestic coordination;
- pursue money laundering, terrorist financing and the financing of proliferation;
- apply preventive measures for the financial sector and other designated sectors;
- establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures;
- enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
- facilitate international cooperation.

The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug-money laundering. In October 2001 the FATF expanded its mandate to deal with the issue of the funding of terrorist acts and terrorist organisations, and took the important step of creating the Eight (later expanded to Nine) Special Recommendations on Terrorist Financing. The FATF Recommendations were revised a second time in 2003, and these, together with the Special Recommendations, have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).

Following the conclusion of the third round of mutual evaluations of its members, the FATF has reviewed and updated the FATF Recommendations, in close co-operation with the FATF-Style Regional Bodies (FSRBs) and the observer organisations, including the International Monetary Fund, the World Bank and the United Nations. The revisions address new and emerging threats, clarify and strengthen many of the existing obligations, while maintaining the necessary stability and rigour in the Recommendations.

The FATF Standards have also been revised to strengthen the requirements for higher risk situations, and to allow countries to take a more focused approach in areas where high risks remain or implementation could be enhanced. Countries should first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk.

The risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way.

Combating terrorist financing is a very significant challenge. An effective AML/CFT system, in general, is important for addressing terrorist financing, and most measures previously focused on terrorist financing are now integrated throughout the Recommendations, therefore obviating the need for the Special Recommendations. However, there are some Recommendations that are unique to terrorist financing, which are set out in Section C of the FATF Recommendations. These are: Recommendation 5 (the criminalisation of terrorist financing); Recommendation 6 (targeted financial sanctions related to terrorism & terrorist financing); and Recommendation 8 (measures to prevent the misuse of non-profit organisations). The proliferation of

weapons of mass destruction is also a significant security concern, and in 2008 the FATF's mandate was expanded to include dealing with the financing of proliferation of weapons of mass destruction. To combat this threat, the FATF has adopted a new Recommendation (Recommendation 7) aimed at ensuring consistent and effective implementation of targeted financial sanctions when these are called for by the UN Security Council.

The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary. The measures set out in the FATF Standards should be implemented by all members of the FATF and the FSRBs, and their implementation is assessed rigorously through Mutual Evaluation processes, and through the assessment processes of the International Monetary Fund and the World Bank – on the basis of the FATF's common assessment methodology. Some Interpretive Notes and definitions in the glossary include examples which illustrate how the requirements could be applied. These examples are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

The FATF also produces Guidance, Best Practice Papers, and other advice to assist countries with the implementation of the FATF standards. These other documents are not mandatory for assessing compliance with the Standards, but countries may find it valuable to have regard to them when considering how best to implement the FATF Standards. A list of current FATF Guidance and Best Practice Papers, which are available on the FATF website, is included as an annex to the Recommendations.

The FATF is committed to maintaining a close and constructive dialogue with the private sector, civil society and other interested parties, as important partners in ensuring the integrity of the financial system. The revision of the Recommendations has involved extensive consultation, and has benefited from comments and suggestions from these stakeholders. Going forward and in accordance with its mandate, the FATF will continue to consider changes to the standards, as appropriate, in light of new information regarding emerging threats and vulnerabilities to the global financial system.

The FATF calls upon all countries to implement effective measures to bring their national systems for combating money laundering, terrorist financing and the financing of proliferation into compliance with the revised FATF Recommendations.

INTRODUCTION TO METHODOLOGY

1. This document provides the basis for undertaking assessments of technical compliance with the revised FATF Recommendations, adopted in February 2012, and for reviewing the level of effectiveness of a country's Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) system. It consists of three sections. This first section is an introduction, giving an overview of the assessment Methodology[4], 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 4th round of mutual evaluations, the FATF has adopted complementary approaches for assessing technical compliance with the FATF Recommendations, and for assessing whether and how the AML/CFT 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 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 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 and how successful it is in maintaining a strong AML/CFT system, as required by the FATF Recommendations.

4. This Methodology is designed to assist assessors when they are conducting an assessment of a country's compliance with the international AML/CFT 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 AML/CFT 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 different Recommendations (e.g., the makeup of its economy and its financial sector);
- *structural elements* which underpin the AML/CFT system; and
- *other contextual factors* which could influence the way AML/CFT measures are implemented and how effective they are.

6. The 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 factors to the country at the outset of the

[4] 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).

assessment, and throughout the assessment process. Relevant factors can 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

7. 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. Assessors should also note the guidance in paragraph 16, 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).

8. Assessors should also consider issues of *materiality*, including, for example, the relative importance of different parts of the financial sector and different DNFBPs; the size, integration and make-up of the financial sector; 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 or cultural 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 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 effectiveness, as set out below.

9. An effective AML/CFT 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 lack of such structural elements, or significant weaknesses and shortcomings in the general framework, may significantly hinder the implementation of an effective AML/CFT framework; and, where assessors identify a lack of compliance or effectiveness, missing structural elements may be a reason for this and should be identified in the MER, where relevant.

10. *Other contextual factors* that might significantly influence the effectiveness of a country's AML/CFT measures include the maturity and sophistication of the regulatory and supervisory regime in the country; the level of corruption and the impact of measures to combat corruption; or the level of financial exclusion. Such factors may affect the ML/FT risks and increase or reduce the effectiveness of AML/CFT measures.

11. Assessors should consider the contextual factors above, including the risks, issues of materiality, structural elements, and other contextual factors, to reach a general understanding of the context in which the country's AML/CFT system operates. These factors may 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. Based on these elements the assessors should make their own judgement of the context in which the country's AML/CFT system operates, and should make this analysis clear and explicit in the MER.

12. 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.

GENERAL INTERPRETATION AND GUIDANCE

13. A full set of definitions from the FATF Recommendations are included in the Glossary which accompanies the Recommendations. Assessors should also take note of the following guidance on other points of general interpretation, which is important to ensure consistency of approach.

14. **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

15. **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 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.[5] See the Note to Assessors in R.15 for more detailed guidance.

16. **Evaluating the country's Assessment of risk** – Assessors are not expected to conduct an independent risk assessment of their own when assessing Recommendation1 and Immediate Outcome 1, 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.

17. When assessing Recommendation 1, assessors should concentrate their analysis on the following elements: (1) processes and mechanisms in place to produce and coordinate the risk assessment(s); (2) the reasonableness of the risk assessment(s); and, (3) the alignment of risk-based measures with the risks identified (e.g., exemptions, higher or lower risks situations).

18. When assessing Immediate Outcome 1, assessors, based on their views of the reasonableness of the assessment(s) of risks, should focus on how well the competent authorities use their understanding of the risks in practice to inform policy development and activities to mitigate the risks.

19. **Risk-based requirements** – For each Recommendation where financial institutions and Designated Non-Financial Businesses or Professions (DNFBPs) should be required to take certain actions, assessors should normally assess compliance on the basis that all financial institutions 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

[5] 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.

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 there are deficiencies in a country's preventive measures, and their importance. 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.

20. **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 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.

21. **Requirements fo 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 (DNFBPs and VASPs) should be required"*.

22. **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. 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).

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

24. **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") 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 Outcome 11, except those on national co-operation and co-ordination, which are included in Immediate Outcome 1. Issues relating to the financing of proliferation should be considered in those places only, and not in other parts of the assessment.

25. **National, supra-national and sub-national measures** – In some countries, AML/CFT issues are addressed not just at the level of the national government, but also at state/province or local levels. When assessments are being conducted, appropriate steps should be taken to ensure that AML/CFT measures at the state/provincial level are also adequately considered. Equally, assessors should take into account and refer to supra-national laws or regulations that apply to a country. Annex I sets out the specific Recommendations that may be assessed on a supra-national basis.

26. **Financial Supervision** – Laws and enforceable means that impose preventive AML/CFT 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. 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, it will vary from country to country as to whether these laws and obligations are implemented and enforced through a regulatory or supervisory framework, or by other means.

27. **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[6]. In the effectiveness assessment, assessors should consider whether the sanctions applied in practice are *effective* at ensuring future compliance by the sanctioned institution; and *dissuasive* of non-compliance by others.

28. **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.

29. **Draft legislation and proposals** – Assessors should only take into account relevant laws, regulations or other AML/CFT 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.

30. **FATF Guidance** - assessors may also consider FATF Guidance as background information on how countries can 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, but the application of the guidance should not form part of the assessment.

---

[6] 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

31. 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.

32. 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 may differ from one country to the next. Provided the FATF Recommendations are complied with, countries are entitled to implement the FATF Standards[7] 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 the risks, and the structural or contextual factors for the country.

33. 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

34. 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 or not met.

35. It is essential to note that it is the responsibility of the assessed country to demonstrate that its AML/CFT 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.

36. **Weighting** – 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

[7] The FATF Standards comprise the FATF Recommendations and their Interpretive Notes.

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.

37. **Overlaps between Recommendations** – In many cases the same underlying deficiency will have a cascading effect on the assessment of several different Recommendations. 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 should also clearly indicate in the MER that the same underlying cause is involved in all relevant Recommendations.

38. **Comparison with previous ratings** – Due to the revision and consolidation of the FATF Recommendations and Special Recommendations in 2012, and the introduction of separate assessments for technical compliance and effectiveness, the ratings given under this Methodology will not be directly comparable with ratings given under the 2004 Methodology.

EFFECTIVENESS

39. The assessment of the effectiveness of a country's AML/CFT 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 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*".

40. In the AML/CFT 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.

41. The goal of an assessment of effectiveness is to provide an appreciation of the whole of the country's AML/CFT 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 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.

42. It is essential to note that it is the responsibility of the assessed country to demonstrate that its AML/CFT 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

43. 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 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 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 system should achieve, and they feed into three Intermediate Outcomes which represent the major thematic goals of AML/CFT 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.

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

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.

Intermediate Outcomes:	*Immediate Outcomes:*
Policy, coordination and cooperation mitigate the money laundering and financing of terrorism risks.	1. Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation. 2. International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets. 3. Supervisors appropriately supervise, monitor and regulate financial institutions, DNFBPs and VASPs for compliance with AML/CFT requirements commensurate with their risks. 4. Financial institutions, DNFBPs and VASPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions. 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. 6. Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations 7. Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions. 8. Proceeds and instrumentalities of crime are confiscated. 9. Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions. 10. Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector. 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.
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.	
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.	

SCOPING

45. 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 10 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

46. 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 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 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.

47. 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, material or contextual factors; particularities of the country's laws and institutions; or if the country applies compensatory AML/CFT 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

48. 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 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, 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, where possible, make recommendations to improve its ability to achieve the specific outcome. They should base their analysis and recommendations on their consideration of the *core issues* 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 there may still be value in identifying good practises or potential further improvements, or ongoing efforts needed to sustain a high level of effectiveness).

Characteristics of an Effective System

49. 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

50. 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*.

51. 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 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

52. 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.

53. 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.

54. 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 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

55. 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 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.

56. 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.

57. 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.

58. 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

59. 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 Outcome 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.

CONCLUSIONS ON EFFECTIVENESS

60. 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.

61. ***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 not 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.

62. Assessors' conclusions should reflect only *whether the outcome is being achieved*. Assessors should set-aside their own preferences about the best way to achieve effectiveness, and 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.

63. ***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.,* problems or weaknesses 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.

64. 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 SYSTEM

65. 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 system, including both the level of effectiveness and the level of technical compliance. The report should prioritise these recommendations for remedial measures, taking into account the country's circumstances and capacity, 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 measures in order to most effectively mitigate the risks the country faces. 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.

66. 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 system, and that their own preferred model may not be appropriate in the context of the country assessed.

67. 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 recommendations (*e.g.,* on the scheduling of certain measures), so as not to hinder countries efforts to fully adapt the recommendations to fit local circumstances.

68. 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.

POINT OF REFERENCE

69. 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.

LEGAL BASIS OF REQUIREMENTS ON FINANCIAL INSTITUTIONS AND DNFBPS

1. All requirements for financial institutions or DNFBPs 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 non-compliance. 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 and DNFBPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

COMBINED FATF RECOMMENDATIONS AND METHODOLOGY

A. AML/CFT POLICIES AND COORDINATION

RECOMMENDATION 1	ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH[8]

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should also identify, assess, and understand the proliferation financing risks for the country. 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. Countries should take commensurate action aimed at ensuring that these risks are mitigated effectively, including designating an authority or mechanism to coordinate actions to assess risks, and allocate resources efficiently for this purpose. Where countries identify higher risks, they should ensure that they adequately address such risks. Where countries identify lower risks, they should ensure that the measures applied are commensurate with the level of proliferation financing risk, while still ensuring full implementation of the targeted financial sanctions as required in Recommendation 7.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering, terrorist financing and proliferation financing risks.

Main Criteria

OBLIGATIONS AND DECISIONS FOR COUNTRIES

Risk assessment

1.1. Countries[9] 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.

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.

---

[8] 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.

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

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.[10]

1.9. Supervisors and SRBs should ensure that financial institutions and DNFBPs are implementing their obligations under Recommendation 1.[11]

OBLIGATIONS AND DECISIONS FOR FINANCIAL INSTITUTIONS AND DNFBPS

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)[12]. 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.

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.

INTERPRETIVE NOTE TO RECOMMENDATION 1 (ASSESSING ML/TF RISKS AND APPLYING A RISK-BASED APPROACH)

---

[10] 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.

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

[12] 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.

1. The risk-based approach (RBA) is an effective way to combat money laundering and terrorist financing. In determining how the RBA should be implemented in a sector, countries should consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of the relevant sector. Countries should understand that the discretion afforded, and responsibility imposed on, financial institutions and designated non-financial bodies and professions (DNFBPs) by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.

2. In implementing a RBA, financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. Specific Recommendations set out more precisely how this general principle applies to particular requirements. Countries may also, in strictly limited circumstances and where there is a proven low risk of money laundering and terrorist financing, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP (see below). Equally, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from money laundering and terrorist financing, and which do not fall under the definition of financial institution or DNFBP, they should consider applying AML/CFT requirements to such sectors.

ASSESSING PROLIFERATION FINANCING RISKS AND APPLYING RISK-BASED MEASURES

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 sanctions obligations referred to in Recommendation 7.[13] These obligations set out in Recommendation 7 place strict requirements on all natural and legal persons, which are not risk-based. In the context of proliferation financing risk, risk-based measures by financial institutions and DNFBPs seek to reinforce and complement the full implementation of the strict requirements of Recommendation 7, by detecting and preventing the non-implementation, potential breach, or evasion of targeted financial sanctions. In determining the measures to mitigate proliferation financing risks in a sector, countries should consider the proliferation financing risks associated with the relevant sector. By adopting risk-based measures, competent authorities, financial institutions and DNFBPs should be able to ensure that these measures are commensurate with the risks identified, and that would enable them to make decisions on how to allocate their own resources in the most effective way.

4. Financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate proliferation financing risks.[14] This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. Countries should ensure full implementation of Recommendation 7 in any risk scenario. Where there are higher risks, countries should require financial institutions and DNFBPs to take commensurate measures to manage and mitigate the risks. Where the risks are lower, they should ensure that the measures applied are

[13] Paragraphs 1 and 2 of the Interpretive Note to Recommendation 7, and the related footnotes, set out the scope of Recommendation 7 obligations; including that it is limited to targeted financial sanctions and does not cover other requirements of the UNSCRs. The requirements of the FATF Standards relating to proliferation financing are limited to Recommendations 1, 2, 7 and 15 only. The requirements under Recommendation 1 for PF risk assessment and mitigation, therefore, do not expand the scope of other requirements under other Recommendations.

[14] Countries may decide to exempt a particular type of financial institution or DNFBP from the requirements to identify, assess, monitor, manage and mitigate proliferation financing risks, provided there is a proven low risk of proliferation financing relating to such financial institutions or DNFBPs. However, full implementation of the targeted financial sanctions as required by Recommendation 7 is mandatory in all cases.

commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

A. Obligations and decisions for countries

ML/TF risks

5. **Assessing ML/TF risk** – Countries[15] should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

6. **Higher risk** – Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks, and, without prejudice to any other measures taken by countries to mitigate these higher risks, either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately. 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.

7. **Lower risk** – Countries may decide to 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 money laundering and terrorist financing risks, as referred to in paragraph 3.

   Independent of any decision to specify certain lower risk categories in line with the previous paragraph, countries may also allow financial institutions and DNFBPs to apply simplified customer due diligence (CDD) measures, provided that the requirements set out in section B below ("Obligations and decisions for financial institutions and DNFBPs"), and in paragraph 7 below, are met.

8. **Exemptions** – Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided:

   a) there is a proven low risk of money laundering and terrorist financing; this 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 low risk of money laundering and terrorist financing.

   While the information gathered may vary according to the level of risk, the requirements of Recommendation 11 to retain information should apply to whatever information is gathered.

9. **Supervision and monitoring of risk** – Supervisors (or SRBs for relevant DNFBPs sectors) should ensure that financial institutions and DNFBPs are effectively implementing the obligations set out below. When carrying out this function, supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles and risk assessments prepared by financial institutions and DNFBPs, and take the result of this review into consideration.

---

[15] Where appropriate, AML/CFT risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

PF risk

10. **Assessing PF risk** - Countries[16] should take appropriate steps to identify and assess the proliferation financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's CPF regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of CPF resources by competent authorities; and (iii) make information available for PF risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and SRBs, financial institutions and DNFBPs.

11. **Mitigating PF risk** - Countries should take appropriate steps to manage and mitigate the proliferation financing risks that they identify. Countries should develop an understanding of the means of potential breaches, evasion and non-implementation of targeted financial sanctions present in their countries that can be shared within and across competent authorities and with the private sector. Countries should ensure that financial institutions and DNFBPs take steps to identify circumstances, which may present higher risks and ensure that their CPF regime addresses these risks. Countries should ensure full implementation of Recommendation 7 in any risk scenario. Where there are higher risks, countries should require financial institutions and DNFBPs to take commensurate measures to manage and mitigate these risks. Correspondingly, where the risks are lower, they should ensure that the measures applied are commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

B. Obligations and decisions for financial institutions and DNFBPs

ML/TF risks

12. **Assessing MF/TF risk** – Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of money laundering and terrorist financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their money laundering and terrorist financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

13. **Risk management and mitigation** – Financial institutions and DNFBPs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution or DNFBP). They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs.

14. **Higher risk** – Where higher risks are identified financial institutions and DNFBPs should be required to take enhanced measures to manage and mitigate the risks.

15. **Lower risk** – Where lower risks are identified, countries may allow financial institutions and DNFBPs to take simplified measures to manage and mitigate those risks.

16. When assessing risk, financial institutions and DNFBPs should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Financial institutions and DNFBPs may differentiate the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

---

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

PF risk

17. **Assessing PF risk** - Financial institutions and DNFBPs should be required to take appropriate steps, to identify and assess their proliferation financing risks. This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of proliferation financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their proliferation financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

18. **Mitigating PF risk** - Financial institutions and DNFBPs should have policies, controls and procedures to manage and mitigate effectively the risks that have been identified. This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs. Countries should ensure full implementation of Recommendation 7 in any risk scenario. Where there are higher risks, countries should require financial institutions and DNFBPs to take commensurate measures to manage and mitigate the risks (i.e. introducing enhanced controls aimed at detecting possible breaches, non-implementation or evasion of targeted financial sanctions under Recommendation 7). Correspondingly, where the risks are lower, they should ensure that those measures are commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

RECOMMENDATION 2	NATIONAL COOPERATION AND COORDINATION

Countries should have national AML/CFT/CPF policies, informed by the risks[17] identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination 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).

Main Criteria

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

2.2. Countries should designate an authority or have a co-ordination or other mechanism that is responsible for national AML/CFT policies.

2.3. Mechanisms should be in place to enable policy makers, the Financial Intelligence Unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities to co-operate, and where appropriate, co-ordinate and exchange information domestically with each other concerning the development and implementation of AML/CFT policies and activities. Such mechanisms should apply at both policymaking and operational levels.

2.4. Competent authorities should have similar co-operation and, where appropriate, coordination mechanisms to combat the financing of proliferation of weapons of mass destruction.

2.5. Countries should have cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).[18]

INTERPRETIVE NOTE TO RECOMMENDATION 2

1. Countries should establish appropriate inter-agency frameworks for co-operation and coordination with respect to combating money laundering, terrorist financing and the financing of proliferation. These may be a single framework or different frameworks for ML, TF and PF respectively.
2. Such frameworks should be led by one or more designated authorities, or another mechanism that is responsible for setting national policies and ensuring co-operation and co-ordination among all the relevant agencies.
3. Inter-agency frameworks should include the authorities relevant to combating ML, TF and PF. Depending on the national organisation of functions, authorities relevant to such frameworks could include:
   a) The competent central government departments (e.g. finance, trade and commerce, home, justice and foreign affairs);
   b) Law enforcement, asset recovery and prosecution authorities;

[17] 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.

[18] 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.

c) Financial intelligence unit;

d) Security and Intelligence agencies;

e) Customs and border authorities;

f) Supervisors and self-regulatory bodies;

g) Tax authorities;

h) Import and export control authorities;

i) Company registries, and where they exist, beneficial ownership registries; and

j) Other agencies, as relevant.

4. Countries should ensure that there are mechanisms in place to permit effective operational cooperation, and where appropriate, co-ordination and timely sharing of relevant information domestically between different competent authorities for operational purposes related to AML, CFT and CPF, both proactive and upon request. These could include: (a) measures to clarify the role, information needs and information sources of each relevant authority; (b) measures to facilitate the timely flow of information among relevant authorities (e.g. standard formats and secure channels), and (c) practical mechanisms to facilitate inter-agency work (e.g. joint teams or shared data platforms).

B. MONEY LAUNDERING AND CONFISCATION

RECOMMENDATION 3	MONEY LAUNDERING OFFENCE

Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

Main Criteria

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)[19].

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[20].

3.3. Where countries apply a threshold approach or a combined approach that includes a threshold approach[21], 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.

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.

---

[19] Note in particular the physical and material elements of the offence.

[20] 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.

[21] 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.

INTERPRETIVE NOTE TO RECOMMENDATION 3 (MONEY LAUNDERING OFFENCE)

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

2. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences; or 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 to a list of predicate offences; or a combination of these approaches.

3. Where countries apply a threshold approach, predicate offences should, at a minimum, comprise all offences that fall within the category of serious offences under their national law, or should include offences that are punishable by a maximum penalty of more than one year's imprisonment, or, for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences that are punished by a minimum penalty of more than six months imprisonment.

4. Whichever approach is adopted, each country should, at a minimum, include a range of offences within each of the designated categories of offences. The offence of money laundering should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.

5. 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. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence, had it occurred domestically.

6. Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

7. Countries should ensure that:

   a) The intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances.

   b) Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of money laundering.

   c) 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 effective, proportionate and dissuasive.

   d) There should be appropriate ancillary offences to the offence of money laundering, including participation in, association with or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

RECOMMENDATION 4	CONFISCATION AND PROVISIONAL MEASURES

Countries should ensure that they have policies and operational frameworks that prioritise asset recovery in both the domestic and international context.

Taking into account the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption, and the Terrorist Financing Convention, countries should have measures, including legislative measures, to enable their competent authorities to:

a) identify, trace and evaluate criminal property and property of corresponding value;

b) suspend or withhold consent to a transaction;

c) take any appropriate investigative measures;

d) expeditiously carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of criminal property and property of corresponding value;

e) confiscate criminal property and property of corresponding value through conviction- based confiscation;

f) confiscate criminal property through non-conviction based confiscation;

g) enforce a resulting confiscation order; and

h) ensure effective management of property that is frozen, seized or confiscated.

Main Criteria

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[22];

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.

[22] 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.

INTERPRETIVE NOTE TO RECOMMENDATION 4 (CONFISCATION AND PROVISIONAL MEASURES)

A. Prioritisation and asset recovery frameworks

1. Countries should review their asset recovery regime to ensure its ongoing effectiveness and provide sufficient resources to effectively pursue asset recovery.

2. Consistent with Recommendation 2, countries should ensure that they have the necessary domestic cooperation and coordination frameworks and agency structures to enable effective use of the measures below.

B. Criminal property and property of corresponding value

3. Criminal property and property of corresponding value extends to property owned or held by third parties, but without prejudicing the rights of bona fide third parties. Examples of circumstances where property is owned or held by non-bona fide third parties and could be criminal property or property of corresponding value include:

   (a) property under the effective control of the defendant or person under investigation and, for example, held or owned by family members, associates or legal persons and arrangements; or

   (b) where the property has been gifted or transferred to the third party for an amount significantly above or below market value.

C. Provisional measures

4. In response to relevant information, countries should enable the FIU or other competent authority to take immediate action, directly or indirectly, to withhold consent to or suspend a transaction suspected of being related to money laundering, predicate offences, or terrorist financing. The maximum duration of this measure should be specified and allow sufficient time to analyse the transaction and for competent authorities to initiate, where appropriate, an action to freeze or seize.

5. Countries should have measures, including legislative measures, to enable their competent authorities to expeditiously carry out provisional measures. This should include:

   (a) allowing the initial application to freeze or seize criminal property and property of corresponding value to be made ex parte or without prior notice;[23] and

   (b) ensuring that provisional measures do not have unreasonable or unduly restrictive conditions for effective action, such as in relation to demonstrating the risk of dissipation

[23] *Ex parte* proceedings may be subject to appropriate safeguards under domestic law, including the triggering of notice or an i*nter partes* review after the implementation of the provisional measure.

6. When necessary to act as expeditiously as possible, countries should enable competent authorities to freeze and seize criminal property and property of corresponding value without a court order, with such action reviewable through judicial proceedings within a period of time. If either or both freezing or seizing without a court order is inconsistent with fundamental principles of domestic law, a country may use an alternative mechanism if it enables their competent authorities to systematically take action quickly enough to prevent the dissipation of criminal property and property of corresponding value.

7. Countries should have measures, including legislative measures, that enable their competent authorities to take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or confiscate criminal property and property of corresponding value.

D. Confiscation

8. Countries need a comprehensive range of measures, including legislative measures, available to confiscate criminal property and property of corresponding value, including those measures in paragraphs (9)-(13) below. Which measures, or combination of measures, will be applied depends on the circumstances of the case. It is also important for such measures to be implemented in a manner which respects the substantive and procedural rights and safeguards that may be implicated by confiscation.

9. Countries should have measures, including legislative measures, to enable the confiscation of criminal property and property of corresponding value following the conviction of a person.

10. To the extent that such a requirement is consistent with fundamental principles of domestic law, countries should have measures, including legislative measures, which enable confiscation to be extended to other property of a person convicted of money laundering, predicate offences,[24] or terrorism financing where the court is satisfied that such property is derived from criminal conduct.[25]

11. Countries should have measures, including legislative measures, to enable the confiscation of criminal property without requiring a criminal conviction (non-conviction based confiscation) in relation to a case involving money laundering, predicate offences[26] or terrorism financing, to the extent that such a requirement is consistent with fundamental principles of domestic law. Countries have flexibility in how they implement non-conviction based confiscation.

12. Countries should consider adopting measures which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation.

E. Asset recovery and tax authorities

13. Countries should enable their competent authorities and tax authorities to cooperate and, where appropriate, coordinate and share information domestically with a view to enhancing asset recovery efforts and supporting the identification of criminal property. This could, in

[24] Countries may limit the application of extended confiscation to serious offences consistent with Recommendation 3.

[25] In determining whether the property in question is derived from criminal conduct, this could include, for example, whether the value of the property represents the proceeds of a criminal lifestyle or is disproportionate to the lawful income of the convicted person.

[26] Countries may limit the application of non-conviction based confiscation to serious offences consistent with Recommendation 3.

appropriate cases, where there is a tax liability, support the recovery of such liabilities by the tax authorities.

F. Asset management, return and disposal

14. Countries should have effective mechanisms for managing, preserving, and, when necessary, disposing of, frozen, seized, or confiscated property. Preservation of the value of property should include the pre-confiscation sale of property, where appropriate.

15. Countries should consider establishing an asset recovery fund into which all, or a portion of, confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

16. Countries should ensure that they have measures that enable them to enforce a confiscation order and realise the property or value subject to the confiscation order, leading to the permanent deprivation of the property or value subject to the order.

17. Countries should have mechanisms to return confiscated property to its prior legitimate owners or to use it to compensate victims of crime.

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

RECOMMENDATION 5	TERRORIST FINANCING OFFENCE

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

Main Criteria

5.1. Countries should criminalise TF on the basis of the Terrorist Financing Convention[27].

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).[28]

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.

5.8. It should also be an offence to:

a) attempt to commit the TF offence;

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

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

d) 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[29].

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.

---

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

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

[29] 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.

INTERPRETIVE NOTE TO RECOMMENDATION 5 (TERRORIST FINANCING OFFENCE)

A. OBJECTIVES

1. Recommendation 5 was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and, *inter alia*, money laundering, another objective of Recommendation 5 is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering.

B. CHARACTERISTICS OF THE TERRORIST FINANCING OFFENCE

2. Terrorist financing 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); (b) by a terrorist organisation; or (c) by an individual terrorist.

3. Terrorist financing includes 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.

4. Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy is not sufficient to comply with this Recommendation.

5. Terrorist financing offences should extend to any funds or other assets, whether from a legitimate or illegitimate source.

6. Terrorist financing 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).

7. Countries should ensure that the intent and knowledge required to prove the offence of terrorist financing may be inferred from objective factual circumstances.

8. Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of terrorist financing.

9. 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 effective, proportionate and dissuasive.

10. It should also be an offence to attempt to commit the offence of terrorist financing.

11. It should also be an offence to engage in any of the following types of conduct:

    a) Participating as an accomplice in an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

    b) Organising or directing others to commit an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

    c) Contributing to the commission of one or more offence(s), as set forth in paragraphs 2 or 9 of this Interpretive Note, by a group of persons acting with a common purpose. 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 terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.

12. Terrorist financing 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.

RECOMMENDATION 6	TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

Main criteria

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[30]; a statement of case[31] which contains as much detail as possible on the basis for the listing[32]; 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[33];

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

[30] 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.

[31] 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).

[32] 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.

[33] 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)

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[34]. 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

6.4. Countries should implement targeted financial sanctions without delay.[35]

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[36] 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.

---

[34] 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.

[35] 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.

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

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.

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;[37]

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 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.

[37] 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.

INTERPRETIVE NOTE TO RECOMMENDATION 6
(TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING)

A. OBJECTIVE

1. Recommendation 6 requires each country to implement targeted financial sanctions to comply with the United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of: (i) any person[38] or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, as required by Security Council resolution 1267 (1999) and its successor resolutions[39]; or (ii) any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).

2. It should be stressed that none of the obligations in Recommendation 6 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by Recommendation 4 (confiscation and provisional measures)[40]. Measures under Recommendation 6 may complement criminal proceedings against a designated person or entity, and be adopted by a competent authority or a court, but are not conditional upon the existence of such proceedings. Instead, the focus of Recommendation 6 is on the preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to terrorist groups; and the use of funds or other assets by terrorist groups. In determining the limits of, or fostering widespread support for, an effective counter-terrorist financing regime, countries must also respect human rights, respect the rule of law, and recognise the rights of innocent third parties.

B. IDENTIFYING AND DESIGNATING PERSONS AND ENTITIES FINANCING OR SUPPORTING TERRORIST ACTIVITIES

3. For resolution 1267 (1999) and its successor resolutions, designations relating to Al-Qaida are made by the 1267 Committee, and designations pertaining to the Taliban and related threats to Afghanistan are made by the 1988 Committee, with both Committees acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), designations are made, at the national or supranational level, by a country or countries acting on their 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 resolution 1373 (2001), as set forth in Section E.

4. Countries need to have the authority, and effective procedures or mechanisms, to identify and initiate proposals for designations of persons and entities targeted by resolution 1267 (1999) and its successor resolutions, consistent with the obligations set out in those Security Council resolutions[41]. Such authority and procedures or mechanisms are essential to propose persons and entities to the Security Council for designation in accordance with Security Council listbased programmes, pursuant to those Security Council

---

38 Natural or legal person.

39 Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are resolutions: 1333 (2000), 1363 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

40 Based on requirements set, for instance, in the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)(the Vienna Convention) and the United Nations Convention against Transnational Organised Crime (2000) (the Palermo Convention), which contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Additionally, the International Convention for the Suppression of the Financing of Terrorism (1999)(the Terrorist Financing Convention) contains obligations regarding freezing, seizure and confiscation in the context of combating terrorist financing. Those obligations exist separately and apart from the obligations set forth in Recommendation 6 and the United Nations Security Council Resolutions related to terrorist financing.

41 The relevant Security Council resolutions do not require countries to identify persons or entities and submit these to the relevant United Nations Committees, but to have the authority and effective procedures and mechanisms in place to be able to do so.

resolutions. Countries also need to have the authority and effective procedures or mechanisms to identify and initiate designations of persons and entities pursuant to S/RES/1373 (2001), consistent with the obligations set out in that Security Council resolution. Such authority and procedures or mechanisms are essential to identify persons and entities who meet the criteria identified in resolution 1373 (2001), described in Section E. A country's regime to implement resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), should include the following necessary elements:

a) Countries should identify a competent authority or a court as having responsibility for:

   (i) proposing to the 1267 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1989 (2011) (on Al-Qaida) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria;

   (ii) proposing to the 1988 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1988 (2011) (on the Taliban and those associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria; and

   (iii) designating persons or entities that meet the specific criteria for designation, as set forth in resolution 1373 (2001), as put forward either on the country's own motion or, after examining and giving effect to, if appropriate, 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 resolution 1373 (2001), as set forth in Section E.

b) Countries should have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolution 1988 (2011) and resolution 1989 (2011) and related resolutions, and resolution 1373 (2001) (see Section E for the specific designation criteria of relevant Security Council resolutions). 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 resolution 1373 (2001). To ensure that effective cooperation is developed among countries, countries should ensure that, when receiving a request, they make a prompt determination 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 resolution 1373 (2011), as set forth in Section E.

c) The competent authority(ies) should have appropriate legal authorities and procedures or mechanisms to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

d) When deciding whether or not to make a (proposal for) designation, countries should apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis". For designations under resolutions 1373 (2001), the competent authority of each country will 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. Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding.

e) When proposing names to the 1267 Committee for inclusion on the Al-Qaida Sanctions List, pursuant to resolution 1267 (1999) and its successor resolutions, countries should:

   (i) follow the procedures and standard forms for listing, as adopted by the 1267 Committee;

(ii) provide as much relevant information as possible on the proposed name, 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;

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions); 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. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1267 Committee; and

(iv) specify whether their status as a designating state may be made known.

f) When proposing names to the 1988 Committee for inclusion on the Taliban Sanctions List, pursuant to resolution 1988 (2011) and its successor resolutions, countries should:

(i) follow the procedures for listing, as adopted by the 1988 Committee;

(ii) provide as much relevant information as possible on the proposed name, 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; and

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant designation (see Section E for the specific designation criteria of relevant Security Council resolutions); 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. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1988 Committee.

g) When requesting another country to give effect to the actions initiated under the freezing mechanisms that have been implemented pursuant to resolution 1373 (2001), the initiating country should provide as much detail as possible on: the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

h) Countries should have procedures to be able to operate ex parte against a person or entity who has been identified and whose (proposal for) designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated by the 1267 Committee and 1988 Committee (in the case of resolution 1267 (1999) and its successor resolutions), when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), the obligation for countries to take freezing action and prohibit the dealing in funds or other assets of designated persons and entities, 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 resolution 1373 (2001), as set forth in Section E.

6. Countries should establish the necessary 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[42] 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. This obligation should extend to: 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; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and 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 funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

   b) Countries should prohibit their nationals, or 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 Security Council resolutions (see Section E below).

   c) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance, particularly 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.

   d) Countries should require financial institutions and DNFBPs[43] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by the competent authorities.

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

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of persons and entities designated pursuant to resolution 1267(1999) and its successor resolutions that, in the view of the country, do not or no longer meet the criteria for designation. In the event that the 1267 Committee or 1988 Committee has de-listed a person or entity, the obligation to freeze no longer exists. In the case of de-listing requests related to Al-Qaida, such procedures and criteria should be in accordance with procedures adopted by the 1267 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1989 (2011), and any successor resolutions. In the case of de-listing requests related to the Taliban and related threats to the peace, security and stability of Afghanistan, such procedures and criteria should be in accordance with procedures adopted by the 1988 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and any successor resolutions.

8. For persons and entities designated pursuant to resolution 1373 (2001), countries should have appropriate legal authorities and procedures or mechanisms to delist and unfreeze the funds or other assets of persons and entities that no longer meet the criteria for designation. Countries should also have

---

[42] In the case of the European Union (EU), which is a supra-national jurisdiction under Recommendation 6, the EU law applies as follows. The assets of designated persons and entities are frozen by the EU regulations and their amendments. EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

[43] Security Council resolutions apply to all natural and legal persons within the country.

procedures in place to allow, upon request, review of the designation decision before a court or other independent competent authority.

9. For 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), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

10. Where countries have determined that funds or other assets of persons and entities designated by the Security Council, or one of its relevant sanctions committees, are necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, countries should authorise access to such funds or other assets in accordance with the procedures set out in Security Council resolution 1452 (2002) 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 resolution 1373 (2001) and as set out in resolution 1963 (2010).

11. Countries should provide for a mechanism through which a designated person or entity can challenge their designation, with a view to having it reviewed by a competent authority or a court. With respect to designations on the Al-Qaida Sanctions List, countries should inform designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to resolution 1904 (2009), to accept de-listing petitions.

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

a) **Security Council resolutions 1267 (1999), 1989 (2011) and their successor resolutions[44]:**

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of Al-Qaida, or any cell, affiliate, splinter group or derivative thereof[45] ; or

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i), or by persons acting on their behalf or at their direction.

b) **Security Council resolutions 1267 (1999), 1988 (2011) and their successor resolutions:**

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of those designated and other individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan; or

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(b)(i) of this subparagraph, or by persons acting on their behalf or at their direction.

---

[44] Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999). At the time of issuance of this Interpretive Note, (February 2012) , the successor resolutions to resolution 1267 (1999) are: resolutions 1333 (2000), 1367 (2001), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

[45] OP2 of resolution 1617 (2005) further defines the criteria for being “associated with” Al-Qaida or Usama bin Laden.

c) **Security Council resolution 1373 (2001):**

(i) any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts;

(ii) any entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(c) (i) of this subparagraph; or

(iii) any person or entity acting on behalf of, or at the direction of, any person or entity designated under subsection 13(c) (i) of this subparagraph.

RECOMMENDATION 7	TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

Main criteria

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.[46]

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.

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.

[46] 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.

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[47]. 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 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.

INTERPRETIVE NOTE TO RECOMMENDATION 7 (TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION)

[47] 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.

A. OBJECTIVE

1. Recommendation 7 requires countries to implement targeted financial sanctions[48] to comply with United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, any person[49] or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction.[50]

2. It should be stressed that none of the requirements in Recommendation 7 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by international treaties or Security Council resolutions relating to weapons of mass destruction non-proliferation.[51] The focus of Recommendation 7 is on preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to proliferators or proliferation; and the use of funds or other assets by proliferators or proliferation, as required by the United Nations Security Council (the Security Council).

B. DESIGNATIONS

3. Designations are made by the Security Council in annexes to the relevant resolutions, or by the Security Council Committees established pursuant to these resolutions. There is no specific obligation upon United Nations Member States to submit proposals for designations to the Security Council or the relevant Security Council Committee(s). However, in practice, the Security Council or the relevant Committee(s) primarily depends upon requests for designation by Member States. Security Council resolution 1718 (2006) provides that the relevant Committee shall promulgate guidelines as may be necessary to facilitate the implementation of the measures imposed by this resolution and its successor resolutions. Resolution 2231 (2015) provides that the Security Council shall make the necessary practical arrangements to undertake directly tasks related to the implementation of the resolution.

4. Countries could consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the Security Council for designation in accordance with relevant Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. In this regard, countries could consider the following elements:

   a) identifying a competent authority(ies), either executive or judicial, as having responsibility for:

      (i) proposing to the 1718 Sanctions Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in resolution 1718 (2006)

---

[48] Recommendation 7 is focused on targeted financial sanctions. These include the specific restrictions set out in Security Council resolution 2231 (2015) (see Annex B paragraphs 6(c) and (d)). However, it should be noted that the relevant United Nations Security Council Resolutions are much broader and prescribe other types of sanctions (such as travel bans) and other types of financial provisions (such as activitybased financial prohibitions, category-based sanctions and vigilance measures). With respect to targeted financial sanctions related to the financing of proliferation of weapons of mass destruction and other types of financial provisions, the FATF has issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs.

[49] Natural or legal person.

[50] Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, 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. At the time of issuance of this Interpretive Note (June 2017), the Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) and 2356 (2017). Resolution 2231 (2015), endorsing the Joint Comprehensive Plan of Action, terminated all provisions of resolutions 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.

[51] Based on requirements set, for instance, in the *Nuclear Non-Proliferation Treaty, the Biological and Toxin Weapons Convention, the Chemical Weapons Convention*, and Security Council resolutions 1540 (2004) and 2235 (2016). Those obligations exist separately and apart from the obligations set forth in Recommendation 7 and its interpretive note.

and its successor resolutions[52], if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions); and

(ii) proposing to the Security Council, for designation as appropriate, persons or entities that meet the criteria for designation as set forth in resolution 2231 (2015) and any future successor resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions).

b) having a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolutions 1718 (2006), 2231 (2015), and their successor and any future successor resolutions (see Section E for the specific designation criteria of relevant Security Council resolutions). Such procedures should ensure the determination, according to applicable (supra-)national principles, whether reasonable grounds or a reasonable basis exists to propose a designation.

c) having appropriate legal authority, and procedures or mechanisms, to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

d) when deciding whether or not to propose a designation, taking into account the criteria in Section E of this interpretive note. For proposals of designations, the competent authority of each country will apply the legal standard of its own legal system, taking into consideration human rights, respect for the rule of law, and in recognition of the rights of innocent third parties.

e) when proposing names to the 1718 Sanctions Committee, pursuant to resolution 1718 (2006) and its successor resolutions, or to the Security Council, pursuant to resolution 2231 (2015) and any future successor resolutions, providing as much detail as possible on:

(i) the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and

(ii) specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

f) having procedures to be able, where necessary, to operate ex parte against a person or entity who has been identified and whose proposal for designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated:

a) in the case of resolution 1718 (2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1718 Sanctions Committee of the Security Council[53]; and

b) in the case of resolution 2231 (2015) and any future successor resolutions by the Security Council, when acting under the authority of Chapter VII of the Charter of the United Nations.

---

[52] Recommendation 7 is applicable to all current and future successor resolutions to resolution 1718 (2006). At the time of issuance of this Interpretive Note (June 2017), the successor resolutions to resolution 1718 (2006) are: resolution 1874 (2009), resolution 2087 (2013), resolution 2094 (2013), resolution 2270 (2016), resolution 2321 (2016) and resolution 2356 (2017).

[53] As noted in resolution 2270 (2016) (OP32) this also applies to entities of the Government of the Democratic People's Republic of Korea or the Worker's Party of Korea that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

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

a) Countries[54] 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. This obligation should extend to: 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; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and 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 funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

b) 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 Security Council resolutions (see Section E below).

c) Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance, particularly 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.

d) Countries should require financial institutions and DNFBPs[55] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by competent authorities.

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

f) Countries should adopt appropriate 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.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. 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. Once the Security Council or the relevant Sanctions Committee has de-listed the person or entity, the obligation to freeze no longer exists. In the case of resolution 1718 (2006) and its successor resolutions, such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the Security Council pursuant to resolution 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution. Countries should enable listed persons and entities to petition a request for delisting at the Focal Point for de-listing established pursuant to resolution 1730 (2006), or should inform designated persons or entities to petition the Focal Point directly.

8. For 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), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

---

[54] In the case of the European Union (EU), which is considered a supra-national jurisdiction under Recommendation 7 by the FATF, the assets of designated persons and entities are frozen under EU Common Foreign and Security Policy (CFSP) Council decisions and Council regulations (as amended). EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

[55] Security Council resolutions apply to all natural and legal persons within the country.

9. Where countries have determined that the exemption conditions set out in resolution 1718(2006) and resolution 2231 (2015) are met, countries should authorise access to funds or other assets in accordance with the procedures set out therein.

10. Countries should permit the addition to the accounts frozen pursuant to resolution 1718 (2006) or resolution 2231 (2015) 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.

11. Freezing action taken pursuant to resolution 1737 (2006) and continued by resolution 2231 (2015), or taken pursuant to resolution 2231 (2015), shall 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:

    a) 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 resolution 2231 (2015) and any future successor resolutions;

    b) 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 resolution 2231 (2015); and

    c) 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.[56]

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

    a) **On DPRK - Resolutions 1718 (2006), 2087 (2013), 2094 (2013) and 2270 (2016):**

        (i) any person or entity engaged in the Democratic People's Republic of Korea (DPRK)'s nuclear-related, other WMD-related and ballistic missile-related programmes;

        (ii) any person or entity providing support for DPRK's nuclear-related, other WMDrelated and ballistic missile-related programmes, including through illicit means;

        (iii) any person or entity acting on behalf of or at the direction of any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[57];

        (iv) any legal person or entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[58];

        (v) any person or entity that has assisted in the evasion of sanctions or in violating the provisions of resolutions 1718 (2006) and 1874 (2009);

        (vi) any person or entity that has contributed to DPRK's prohibited programmes, activities prohibited by the DPRK-related resolutions, or to the evasion of provisions; or

---

[56] In cases where the designated person or entity is a financial institution, jurisdictions should consider the FATF guidance issued as an annex to *The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, adopted in June 2013*.

[57] The funds or assets of these persons or entities are frozen regardless of whether they are specifically identified by the Committee. Further, resolution 2270 (2016) OP23 expanded the scope of targeted financial sanctions obligations under resolution 1718 (2006), by applying these to the Ocean Maritime Management Company vessels specified in Annex III of resolution 2270 (2016).

[58] Ibid.

(vii) any entity of the Government of the DPRK or the Worker's Party of Korea, or person or entity acting on their behalf or at their direction, or by any entity owned or controlled by them, that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

b) **On Iran - Resolution 2231 (2015):**

(i) any person or entity having engaged in, directly associated with or provided support for Iran's proliferation sensitive nuclear activities contrary to Iran's commitments in the Joint Comprehensive Plan of Action (JCPOA) or the development of nuclear weapon delivery systems, including through the involvement in procurement of prohibited items, goods, equipment, materials and technology specified in Annex B to resolution 2231 (2015);

(ii) any person or entity assisting designated persons or entities in evading or acting inconsistently with the JCPOA or resolution 2231 (2015); and

(iii) any person or entity acting on behalf or at a direction of any person or entity in subsection 13(b)(i), subsection 13(b)(ii) and/or subsection 13(b)(iii), or by any entities owned or controlled by them.

RECOMMENDATION 8	NON-PROFIT ORGANISATIONS (NPOS)

Countries should identify the organisations which fall within the FATF definition of non-profit organisations (NPOs) and assess their terrorist financing risks. Countries should have in place focused, proportionate and risk-based measures, without unduly disrupting or discouraging legitimate NPO activities, in line with the risk-based approach. The purpose of these measures is to protect such NPOs from terrorist financing abuse, including:

a) by terrorist organisations posing as legitimate entities;

b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and

c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

Main criteria

Taking a risk-based approach

8.1. Countries should:

a) Without prejudice to the requirements of Recommendation 1, since not all NPOs are inherently high risk (and some may represent little or no risk at all), identify which subset of organizations fall within the FATF definition[59] of NPO, and use all relevant sources of information, in order to identify the features and types of NPOs which by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse[60];

b) identify the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs;

c) review the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for terrorism financing support in order to be able to take proportionate and effective actions to address the risks identified; and

d) periodically reassess the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities to ensure effective implementation of measures.

Sustained outreach concerning terrorist financing issues

8.2. Countries should:

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

b) encourage and undertake outreach and educational programmes 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 vulnerabilities and thus protect them from terrorist financing abuse; and

d) encourage NPOs to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

---

[59] 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".

[60] For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

Targeted risk-based supervision or monitoring of NPOs

8.3. Countries should take steps to promote effective supervision or monitoring such that they are able to demonstrate that risk based measures apply to NPOs at risk of terrorist financing abuse.[61]

8.4. Appropriate authorities should:

a) monitor the compliance of NPOs with the requirements of this Recommendation, including the risk-based measures being applied to them under criterion 8.3[62]; and

b) be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.[63]

Effective information gathering and investigation

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 full access to 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.

INTERPRETIVE NOTE TO RECOMMENDATION 8 (NON-PROFIT ORGANISATIONS)

A. INTRODUCTION

1. Given the variety of legal forms that non-profit organisations (NPOs) can have, depending on the country, the FATF has adopted a functional definition of an NPO. This definition is based on those activities and characteristics of an organisation which may put it at risk of TF abuse, rather than on the simple fact that it is operating on a non-profit basis. 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

[61] 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.

[62] In this context, rules and regulations may include rules and standards applied by self-regulatory organisations and accrediting institutions.

[63] 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.

such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works". Without prejudice to Recommendation 1, this Recommendation only applies to those organisations which fall within the FATF definition of an NPO. It does not apply to the entire universe of organisations working in the not-for-profit realm in a country

2. NPOs play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The FATF recognises the vital importance of NPOs in providing these important services, as well as the difficulty of providing assistance to those in need, including in high-risk areas and conflict zones, and applauds the efforts of NPOs to meet such needs. The FATF also recognises the intent and efforts to date of NPOs to promote transparency within their operations and to prevent terrorist financing abuse, including through the development of programmes aimed at discouraging radicalisation and violent extremism.

3. Some NPOs may be at risk of terrorist financing abuse by terrorists for a variety of reasons. NPOs enjoy public trust, which gives some access to considerable sources of funds, and in some contexts are cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, that may be within or near those areas that are most exposed to terrorist activity. In rare cases, terrorist organisations have taken advantage of these and other characteristics to infiltrate NPOs and misuse funds and operations to cover for, or support, terrorist activity. Also, there have been cases where terrorists create sham NPOs or engage in fraudulent fundraising for these purposes. The ongoing international campaign against terrorist financing has identified cases in which terrorists and terrorist organisations exploit some NPOs in the sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations. This misuse not only facilitates terrorist activity, but also undermines the confidence of donors and financial institutions and jeopardises the very integrity of NPOs.

4. Therefore, protecting NPOs from terrorist financing abuse is both a critical component of the global effort to prevent and combat terrorism and a necessary step to preserve the integrity of NPOs, the donor community and the financial institutions they use. Measures to protect NPOs from potential terrorist financing abuse should be focused and in line with the risk-based approach. It is also important for such measures to be implemented in a manner which respects countries' obligations under the Charter of the United Nations and international law, in particular international human rights, international refugee law and international humanitarian law.[64]

B. OBJECTIVES AND GENERAL PRINCIPLES

5. The objective of Recommendation 8 is to ensure that NPOs are not abused by terrorists and terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, includi,ng for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes. In this Interpretive Note, the approach taken to achieve this objective is based on the following general principles:

   a) Past and ongoing terrorist financing abuse of NPOs requires countries to have in place focused, proportionate and risk-based measures in dealing with identified risks. A risk- based approach is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be at risk of terrorist financing abuse, the need to ensure that legitimate NPO activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each country.

   b) Flexibility in developing a national response to terrorist financing abuse of NPOs is essential, in order to allow it to evolve over time as it faces and responds to the changing nature of the terrorist financing threat.

[64] See also UNSC resolution 2462(2019) paras 6 and 23 and UNSC resolution 2664(2022) para.1.

c) Focused, proportionate and risk-based measures adopted by countries to protect NPOs from terrorist financing abuse should not unduly disrupt or discourage legitimate NPO activities, in line with the risk-based approach. Rather, such measures should promote accountability and engender greater confidence among NPOs, across the donor community, the financial institutions and with the general public, that NPO funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of accountability, integrity and public confidence in the management and functioning of NPOs are integral to ensuring they cannot be abused for terrorist financing.

d) Countries should identify and take effective and proportionate action against NPOs that either are exploited by, or are knowingly supporting, terrorists or terrorist organisations, taking into account the specifics of the case. Countries should aim to prevent and prosecute, as appropriate, terrorist financing and other forms of terrorist support. Where NPOs suspected of, or implicated in, terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose must respect the rule of law and should, to the extent reasonably possible, minimise negative impact on innocent and legitimate beneficiaries of NPO activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by NPOs.

e) Countries should develop an understanding of the different degrees of TF risk posed to NPOs and of the corresponding proportionate measures to mitigate these risks in line with the risk-based approach. Many NPOs may face low TF risk exposure, may have adequate self-regulatory measures and related internal control measures to mitigate such risks, and/or may already be subject to adequate levels of legal and regulatory requirements, such that there may be no need for additional measures.[65] Countries should be mindful of the potential impact of measures on legitimate NPO activities and apply them where they are necessary to mitigate the assessed TF risks, without unduly disrupting or discouraging legitimate NPO activities. It is not in line with Recommendation 8 to apply measures to organisations working in the not-for-profit realm to protect them from TF abuse when they do not fall within the FATF's functional definition of NPOs. It is not in line with Recommendation 8 to implement any measures that are not proportionate to the assessed TF risks, and are therefore overly burdensome or restrictive. NPOs are not reporting entities and should not be required to conduct customer due diligence.

f) Developing cooperative relationships among the public and private sectors and with NPOs is critical to understanding NPOs' risks and risk mitigation strategies, raising awareness, increasing effectiveness and fostering capabilities to combat terrorist financing abuse within NPOs. Countries should encourage the development of academic research on, and information-sharing in, NPOs to address terrorist financing related issues.

C. RISK ASSESSMENT AND MITIGATING MEASURES

6. 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. Without prejudice to the requirements of Recommendation 1:

(a) Countries should identify organisations which fall within the FATF definition of NPOs.

(b) Countries should conduct a risk assessment of these NPOs to identify the nature of TF risks posed to them.

(c) Countries should have in place focused, proportionate and risk-based measures to address the TF risks identified, in line with the risk-based approach. Countries may also consider, where they exist, self-regulatory measures and related internal control measures in place within NPOs.

[65] In this context, self-regulatory measures may include rules and standards applied by self-regulatory organisations and accrediting institutions.

(d) These exercises under letters (a) to (c):

(i) should use all relevant and reliable sources of information[66], including through engagement with NPOs,

(ii) could take a variety of forms and may or may not be a written product,

(iii) should be reviewed periodically

D. EFFECTIVE APPROACH IN IDENTIFYING, PREVENTING AND COMBATING TF ABUSE OF NPOS

7. There is a diverse range of approaches in identifying, preventing and combating terrorist financing abuse of NPOs. 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. In other situations, an effective approach should involve all four of the following elements to protect NPOs from potential terrorist financing abuse., without unduly disrupting or discouraging legitimate NPO activities.

a) Sustained outreach concerning terrorist financing issues:

(i) Countries should have clear policies to promote accountability, integrity and public confidence in the administration and management of NPOs.

(ii) Countries should 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.

(iii) Countries should work with NPOs to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect them from terrorist financing abuse.

(iv) Countries should 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.

b) Focused, proportionate and risk-based measures, including oversight or monitoring of NPOs:

Countries should take steps to promote focused, proportionate and risk-based oversight or monitoring of NPOs. A “one-size-fits-all” approach would be inconsistent with the proper implementation of a risk-based approach as stipulated under Recommendation 1 of the FATF Standards. In practice:

(i) Countries should be able to demonstrate that they have in place focused, proportionate and risk-based measures applying to NPOs. It is also possible that existing regulatory and self-regulatory measures and related internal control measures in place within NPOs, or other measures may already sufficiently address the current terrorist financing risk to the NPOs in a country, although terrorist financing risks to the sector should be periodically reviewed.

(ii) Appropriate authorities should monitor the compliance of NPOs with the focused, proportionate and risk-based measures being applied to them.

(iii) Appropriate authorities should be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.[67]

c) Effective information gathering and investigation:

---

[66] For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

[67] The range of such sanctions might include freezing of accounts, removal of trustees, fines, de- certification, de-licensing 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.

(i) Countries should ensure effective cooperation, coordination and information- sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs.

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

(iii) Countries should ensure that access to relevant information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.

(iv) Countries should 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 relevant competent authorities, in order to take preventive or investigative action.

d) Effective capacity to respond to international requests for information about an NPO of concern: consistent with Recommendations on international cooperation, 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.

E. RESOURCES FOR SUPERVISION, MONITORING, AND INVESTIGATION

8. Countries should provide their appropriate authorities, which are responsible for oversight, monitoring and investigation of their NPOs, with adequate financial, human and technical resources.

Glossary of specific terms used in the context of this Recommendation	
Appropriate authorities	refers to competent authorities, including regulators, tax authorities, FIUs, law enforcement, intelligence authorities, accrediting institutions, and potentially self-regulatory organisations in some jurisdictions.
Associate NPOs	includes foreign branches of international NPOs, and NPOs with which partnerships have been arranged.
Beneficiaries	refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.
Non-profit organisation or 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".
Self-regulatory measures	include rules and standards applied by self-regulatory organisations and accrediting institutions.
Terrorist financing abuse	refers to the exploitation by terrorists and terrorist organisations of NPOs to raise or move funds, provide logistical support, encourage or facilitate terrorist recruitment, or otherwise support terrorists or terrorist organisations and operations.

D. PREVENTIVE MEASURES

RECOMMENDATION 9	FINANCIAL INSTITUTION SECRECY LAWS

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

Main criteria

9.1. Financial institution secrecy laws should not inhibit the implementation of the FATF Recommendations.[68]

[68] 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.

CUSTOMER DUE DILIGENCE AND DATA STORAGE

RECOMMENDATION 10	CUSTOMER DUE DILIGENCE[69] (CDD)

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

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) establishing business relations;

(ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) there is a suspicion of money laundering or terrorist financing; or

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

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

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. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), 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 should consider making a suspicious transactions report in relation to the customer.

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

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

Main criteria

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 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[70], the financial institution should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

a) the identity of the natural person(s) (if any[71]) who ultimately has a controlling ownership interest[72] 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[73], 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 payout;

c) for both the above cases – the verification of the identity of the beneficiary should occur at the time of the payout.

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 payout.

Timing of verification

---

[70] 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 majorityowned 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.

[71] 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.

[72] 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%).

[73] 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 payout or when the beneficiary intends to exercise vested rights.

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[74] 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:

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.

INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE)

A. CUSTOMER DUE DILIGENCE AND TIPPING-OFF

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

a) normally seek to identify and verify the identity[75] of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply; and

b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20.

---

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

[75] Reliable, independent source documents, data or information will hereafter be referred to as "identification data."

2. Recommendation 21 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD.

B. CDD – PERSONS ACTING ON BEHALF OF A CUSTOMER

4. When performing elements (a) and (b) of the CDD measures specified under Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person.

C. CDD FOR LEGAL PERSONS AND ARRANGEMENTS

5. When performing CDD measures in relation to customers that are legal persons or legal arrangements[76], financial institutions should be required to identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure. The purpose of the requirements set out in (a) and (b) below, regarding the identification and verification of the customer and the beneficial owner, is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, financial institutions should be required to:

   a) Identify the customer and verify its identity. The type of information that would normally be needed to perform this function would be:

      (i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

      (ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).

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

   b) Identify the beneficial owners of the customer and take reasonable measures[77] to verify the identity of such persons, through the following information:

      (i) For legal persons[78]:

---

[76] In these Recommendations references to legal arrangements such as trusts (or other similar arrangements) being the customer of a financial institution or DNFBP or carrying out a transaction, refers to situations where a natural or legal person that is the trustee establishes the business relationship or carries out the transaction on the behalf of the beneficiaries or according to the terms of the trust. The normal CDD requirements for customers that are natural or legal persons would continue to apply, including paragraph 4 of INR.10, but the additional requirements regarding the trust and the beneficial owners of the trust (as defined) would also apply.

[77] In determining the reasonableness of the identity verification measures, regard should be had to the money laundering and terrorist financing risks posed by the customer and the business relationship.

[78] Measures (i.i) to (i.iii) are not alternative options, but are cascading measures, with each to be used where the previous measure has been applied and has not identified a beneficial owner.

(i.i) The identity of the natural persons (if any – as 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) who ultimately have a controlling ownership interest[79] in a legal person; and

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

(i.iii) Where no natural person is identified under (i.i) or (i.ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

(ii) For legal arrangements:

(ii.i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries[80], and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(ii.ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

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.

D. CDD FOR BENEFICIARIES OF LIFE INSURANCE POLICIES

6. For life or other investment-related insurance business, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

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

b) For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – 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 payout.

The information collected under (a) and/or (b) should be recorded and maintained in accordance with the provisions of Recommendation 11.

7. For both the cases referred to in 6(a) and (b) above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.

8. The beneficiary of a life insurance policy should be included as a relevant risk factor by the financial institution 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, then the

[79] 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%).

[80] For beneficiary(ies) 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 payout or when the beneficiary intends to exercise vested rights.

enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

9. Where a financial institution is unable to comply with paragraphs 6 to 8 above, it should consider making a suspicious transaction report.

E. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED

10. The CDD measures set out in Recommendation 10 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

F. TIMING OF VERIFICATION

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

- Non face-to-face business.
- Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

12. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

G. EXISTING CUSTOMERS

13. Financial institutions should be required to apply CDD measures to existing customers[81] 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.

H. RISK BASED APPROACH[82]

14. The examples below are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

Higher risks

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

a) Customer risk factors:

---

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

[82] The RBA does not apply to the circumstances when CDD should be required but may be used to determine the extent of such measures.

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

b) Country or geographic risk factors:[83]

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

c) Product, service, transaction or delivery channel risk factors:

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions.
- Payment received from unknown or un-associated third parties.

Lower risks

16. There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures.

17. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

a) Customer risk factors:

- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
- Public companies 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.
- Public administrations or enterprises.

b) Product, service, transaction or delivery channel risk factors:

- Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.

[83] Under Recommendation 19 it is mandatory for countries to require financial institutions to apply enhanced due diligence when the FATF calls for such measures to be introduced.

- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

18. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

Risk variables

19. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions undertaken.
- The regularity or duration of the business relationship.

Enhanced CDD measures

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified CDD measures

21. Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified

measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Thresholds

22. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Ongoing due diligence

23. Financial institutions should be required to ensure 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.

RECOMMENDATION 11	**RECORD KEEPING**[84]

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

Main criteria

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.

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

ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

RECOMMENDATION 12	POLITICALLY EXPOSED PERSONS (PEPS)

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;

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

c) take reasonable measures to establish the source of wealth and source of funds; and

d) conduct enhanced ongoing monitoring of the business relationship

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

Main criteria

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.

INTERPRETIVE NOTE TO RECOMMENDATION 12 (POLITICALLY EXPOSED PERSONS)

Financial institutions should take reasonable measures to determine whether the beneficiaries of a life insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. This should occur at the latest at the time of the payout. Where there are higher risks identified, in addition to performing normal CDD measures, financial institutions should be required to:

a) inform senior management before the payout of the policy proceeds; and

b) conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report.

RECOMMENDATION 13	CORRESPONDENT BANKING

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, 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 money laundering or terrorist financing investigation or regulatory action;

b) assess the respondent institution's AML/CFT controls;

c) obtain approval from senior management before establishing new correspondent

d) relationships;

e) clearly understand the respective responsibilities of each institution; and

f) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

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

Main criteria

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.

INTERPRETIVE NOTE TO RECOMMENDATION 13

(CORRESPONDENT BANKING)

The similar relationships to which financial institutions should apply criteria (a) to (e) include, for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

The term *payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

RECOMMENDATION 14	MONEY OR VALUE TRANSFER SERVICES (MVTS)

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

Main criteria

14.1. Natural or legal persons that provide MVTS (MVTS providers) should be required to be licensed or registered.[85]

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.

INTERPRETIVE NOTE TO RECOMMENDATION 14 (MONEY OR VALUE TRANSFER SERVICES)

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 money or value transfer services, and which are already subject to the full range of applicable obligations under the FATF Recommendations.

[85] 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

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

Note to Assessors:

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[86], 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.[87]

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 paragraph 15 of the Introduction section of the Methodology for more guidance on how to assess the FATF Standards relating to virtual assets and VASPs.

Main criteria

[86] 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). See additional guidance in paragraph 15 of the Introduction to the Methodology.

[87] 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[88]

15.3. In accordance with Recommendation 1, countries should:

a) identify and assess the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs;

b) based on their understanding of their risks, 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

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

15.4. Countries should ensure that:

a) VASPs are required to be licensed or registered[89] at a minimum.[90]

(i) when the VASP is a legal person, in the jurisdiction(s) where it is created[91]; and

(ii) when the VASP is a natural person, in the jurisdiction where its place of business is located[92]; 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.[93]

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[94], including systems for ensuring their compliance with national AML/CFT requirements;

---

[88] 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.

[89] 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.

[90] 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.

[91] 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.

[92] 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.

[93] 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.

[94] In this context, a "competent authority" cannot include a SRB.

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

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[95], countries should ensure that:

(i) originating VASPs obtain and hold required and accurate originator information and required beneficiary information[96] on virtual asset transfers, submit[97] 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[98];

(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 cooperation 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.[99]

INTERPRETIVE NOTE TO RECOMMENDATION 15

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

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

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

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

[99] 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.

1. 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." Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs)

2. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks[100] emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should take appropriate steps to manage and mitigate the proliferation financing risks that they identify. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.

3. VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created[101]. In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. 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. 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 in, a VASP. 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.

4. 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.

5. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering and terrorist financing risks emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority (not a SRB), which should conduct risk- based supervision or monitoring. Supervisors should 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 sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.

6. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.

7. With respect to the preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, 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 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information[102] on virtual asset transfers, submit[103]

[100] ''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.

[101] References to creating a legal person include incorporation of companies or any other mechanism that is used.

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

the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that 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. 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. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

8. Countries should rapidly, constructively, and effectively provide the widest possible range of international cooperation 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 exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.

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

RECOMMENDATION 16	WIRE TRANSFERS

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

Main criteria

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[104] 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.

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.

[104] "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.

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[105], 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.

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.

[105] 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.

16.14. For cross-border wire transfers of USD/EUR 1 000 or more[106], 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:

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.

INTERPRETIVE NOTE TO RECOMMENDATION 16 (WIRE TRANSFERS)

A. OBJECTIVE

1. Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available:

a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;

b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and

c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing.

2. To accomplish these objectives, countries should have the ability to trace all wire transfers. Due to the potential terrorist financing threat posed by small wire transfers, countries should minimise thresholds taking into account the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.

---

[106] 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.

B. SCOPE

3. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers , including serial payments, and cover payments.

4. Recommendation 16 is not intended to cover the following types of payments:

   a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction. However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.

   b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

5. Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:

   a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.

   b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.

C. CROSS-BORDER QUALIFYING WIRE TRANSFERS

6. Information accompanying all qualifying wire transfers should always contain:

   a) the name of the originator;

   b) the originator account number where such an account is used to process the transaction;

   c) the originator's address, or national identity number, or customer identification number[107], or date and place of birth;

   d) the name of the beneficiary; and

   e) the beneficiary account number where such an account is used to process the transaction.

7. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

8. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of paragraph 6 in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described in paragraph 7 above), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

D. DOMESTIC WIRE TRANSFERS

9. Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial

[107] The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number referred to in paragraph 7. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.

institution and appropriate authorities by other means. In this latter case, the ordering financial institution need only 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.

10. The information should be made available by the ordering financial institution 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.

E. RESPONSIBILITIES OF ORDERING, INTERMEDIARY AND BENEFICIARY FINANCIAL INSTITUTIONS

Ordering financial institution

11. The ordering financial institution should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information.

12. The ordering financial institution should ensure that cross-border wire transfers below any applicable threshold contain the name of the originator and the name of the beneficiary and an account number for each, or a unique transaction reference number.

13. The ordering financial institution should maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

14. The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above.

Intermediary financial institution

15. For cross-border wire transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

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

17. An intermediary financial institution should take reasonable measures to identify crossborder wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

18. An intermediary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

Beneficiary financial institution

19. A beneficiary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

20. For qualifying wire transfers, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.

21. A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

F. MONEY OR VALUE TRANSFER SERVICE OPERATORS

22. Money or value transfer service (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. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider:

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

Glossary of specific terms used in this Recommendation

Accurate	is used to describe information that has been verified for accuracy.
Batch transfer	is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Beneficiary	refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.
Beneficiary Financial Institution	refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.
Cover Payment	refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
Cross-border wire transfer	refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of *wire transfer* in which at least one of the financial institutions involved is located in a different country.
Domestic wire transfers	refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of *wire transfer* that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country. The term also refers to any chain of *wire transfer* that takes place entirely within the borders of the European Economic Area (EEA)[108].
Intermediary financial institution	refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial

[108] An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of Recommendation 16 compliance.

Glossary of specific terms used in this Recommendation	
	institution.
Ordering financial institution	refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
Originator	refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
Qualifying wire transfers	means a cross-border wire transfer above any applicable threshold as described in paragraph 5 of the Interpretive Note to Recommendation 16.
Required	is used to describe a situation in which all elements of required information are present. Subparagraphs 6(a), 6(b) and 6(c) set out the *required originator information*. Subparagraphs 6(d) and 6(e) set out the *required beneficiary information.*
Serial Payment	refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g. correspondent banks).
Straight-through processing	refers to payment transactions that are conducted electronically without the need for manual intervention.
Unique transaction reference number	refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
Wire transfer	refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.[109]

[109] It is understood that the settlement of wire transfers may happen under a net settlement arrangement. This interpretive note refers to information which must be included in instructions sent from an originating financial institution to a beneficiary financial institution, including through any intermediary financial institution, to enable disbursement of the funds to the recipient. Any net settlement between the financial institutions may be exempt under paragraph 4(b).

RELIANCE, CONTROLS AND FINANCIAL GROUPS

RECOMMENDATION 17	RELIANCE ON THIRD PARTIES

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

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

d) 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.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

Main criteria

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[110] 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

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

INTERPRETIVE NOTE TO RECOMMENDATION 17 (RELIANCE ON THIRD PARTIES)

1. This Recommendation does not apply to outsourcing or agency relationships. In a third-party reliance scenario, the third party should be subject to CDD and record-keeping requirements in line with Recommendations 10 and 11, and be regulated, supervised or monitored. The third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity.
2. For the purposes of Recommendation 17, the term *relevant competent authorities* 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.
3. The term *third parties* means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17.

[110] 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.

RECOMMENDATION 18	INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement groupwide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majorityowned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

Main criteria

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)[111]. Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management[112]; and

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

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.

INTERPRETIVE NOTE TO RECOMMENDATION 18

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

[112] 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.

(INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES)

1. Financial institutions' programmes against money laundering and terrorist financing should include:
   a) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;
   b) an ongoing employee training programme; and
   c) an independent audit function to test the system.
2. The type and extent of measures to be taken should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.
3. Compliance management arrangements should include the appointment of a compliance officer at the management level.
4. Financial groups' programmes against money laundering and terrorist financing should be applicable to all branches and majority-owned subsidiaries of the financial group. These programmes should include measures under (a) to (c) above, and should be appropriate to the business of the branches and majority-owned subsidiaries. Such programmes should be implemented effectively at the level of branches and majority-owned subsidiaries. These programmes should include policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management. Group-level compliance, audit, and/or AML/CFT functions should be provided with 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); and could include an STR, its underlying information, or the fact that an STR has been submitted. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management. Adequate safeguards on the confidentiality and use of information exchanged should be in place, including to prevent tipping-off. Countries may determine the scope and extent of this information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management.
5. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements 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 the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial group, including, as appropriate, requesting the financial group to close down its operations in the host country.

RECOMMENDATION 19	HIGHER-RISK COUNTRIES

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

Main criteria

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.

INTERPRETIVE NOTE TO RECOMMENDATION 19 (HIGHER-RISK COUNTRIES)

1. The enhanced due diligence measures that could be undertaken by financial institutions include those measures set out in paragraph 20 of the Interpretive Note to Recommendation 10, and any other measures that have a similar effect in mitigating risks.
2. Examples of the countermeasures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks:
   a) Requiring financial institutions to apply specific elements of enhanced due diligence.
   b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.
   c) Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.
   d) Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.
   e) Limiting business relationships or financial transactions with the identified country or persons in that country.
   f) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process.
   g) Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.
   h) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned.

i) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries

REPORING OF SUSPICIOUS TRANSACTIONS

RECOMMENDATION 20	REPORTING OF SUSPICIOUS TRANSACTIONS[113]

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

Main criteria

20.1. If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity[114], 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.

INTERPRETIVE NOTE TO RECOMMENDATION 20 (REPORTING OF SUSPICIOUS TRANSACTIONS)

1. The reference to criminal activity in Recommendation 20 refers to all criminal acts that would constitute a predicate offence for money laundering or, at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3. Countries are strongly encouraged to adopt the first of these alternatives.
2. The reference to terrorist financing in Recommendation 20 refers to: the financing of terrorist acts and also terrorist organisations or individual terrorists, even in the absence of a link to a specific terrorist act or acts.
3. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.
4. The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called “indirect reporting”), is not acceptable.

[113] The requirement that financial institutions should report suspicious transactions should be set out in law.

[114] “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

Financial institutions, their directors, officers and employees should be:

a) protected by law from 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, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. These provisions are not intended to inhibit information sharing under Recommendation 18.

Main criteria

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.

DESIGNATED NON-FINANCIAL BUSINESS AND PROFESSIONS

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

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.

c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

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;
- creation, operation 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:

- 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.

Main criteria

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[115] 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[116].

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.

[115] 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.

[116] 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.

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:

- 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.

INTERPRETIVE NOTE TO RECOMMENDATIONS 22 AND 23 (DNFBPS)

1. The designated thresholds for transactions are as follows:

- Casinos (under Recommendation 22) - USD/EUR 3,000
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 22 and 23) - USD/EUR 15,000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

2. The Interpretive Notes that apply to financial institutions are also relevant to DNFBPs, where applicable. For the purposes of R.23, the requirements referring to 'financial groups' in R.18 apply to DNFBP groups operating under the same structure as financial groups. In addition, countries should consider applying the requirements for group-wide programmes to DNFBPs operating in other structures sharing common ownership, management or compliance control to the extent that those structures could better mitigate ML/TF risks by applying group-wide programmes. The type and extent of measures to be taken should be appropriate to the business conducted, the risk of money laundering and terrorist financing and the size of the business. For example, as set out in INR.18, countries may determine the scope and extent of

information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management.

3. To comply with Recommendations 22 and 23, countries do not need to issue laws or enforceable means that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions, so long as these businesses or professions are included in laws or enforceable means covering the underlying activities.

INTERPRETIVE NOTE TO RECOMMENDATION 22 (DNFBPS – CUSTOMER DUE DILIGENCE)

1. Real estate agents should comply with the requirements of Recommendation 10 with respect to both the purchasers and vendors of the property.

2. Casinos should implement Recommendation 10, including identifying and verifying the identity of customers, when their customers engage in financial transactions equal to or above USD/EUR 3,000. 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 customer due diligence information for a particular customer to the transactions that the customer conducts in the casino.

RECOMMENDATION 23	DNFBPS: OTHER MEASURES

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

Main criteria

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 [117] – 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)[118].

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[119].

[117] 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.

[118] 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.

[119] 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.

INTERPRETIVE NOTE TO RECOMMENDATION 23 (DNFBPS – OTHER MEASURES)

1. 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.
2. 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.
3. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of cooperation between these organisations and the FIU.
4. 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.

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

RECOMMENDATION 24	TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS[120]

Countries should assess the risks of misuse of legal persons for money laundering or terrorist financing, and take measures to prevent their misuse. Countries should ensure that there is adequate, accurate and up-to-date information on the beneficial ownership and control of legal persons that can be obtained or accessed rapidly and efficiently by competent authorities, through either a register of beneficial ownership or an alternative mechanism. Countries should not permit legal persons to issue new bearer shares or bearer share warrants, and take measures to prevent the misuse of existing bearer shares and bearer share warrants. Countries should take effective measures to ensure that nominee shareholders and directors are not misused for money laundering or terrorist financing. Countries should consider facilitating access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

Main criteria

24.1. Countries should have mechanisms that identify and describe: (a) the different types, forms and basic features of legal persons in the country; and (b) the processes for the creation of those legal persons, and for obtaining and recording of basic and beneficial ownership information. This information should be publicly available.

24.2. Countries should assess the ML/TF risks associated with all types of legal person created in the country.

Basic Information

24.3. Countries should require that all companies created in a country are registered in a company registry, which should record the company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers, and a list of directors. This information should be publicly available.

24.4. Companies should be required to maintain the information set out in criterion 24.3, and also to maintain a register of their shareholders or members[121], containing the number of shares held by each shareholder and categories of shares (including the nature of the associated voting rights). This information should be maintained within the country at a location notified to the company registry[122].

24.5. Countries should have mechanisms that ensure that the information referred to in criteria 24.3 and 24.4 is accurate and updated on a timely basis.

Beneficial Ownership Information

[120] 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:

1. *Companies* - The measures required by Recommendation 24 are set out with specific reference to companies.
2. *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.
3. *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.

[121] The register of shareholders and members can be recorded by the company itself or by a third person under the company's responsibility.

[122] In cases in which the company or company registry holds beneficial ownership information within the country, the register of shareholders and members need not be in the country, if the company can provide this information promptly on request.

24.6. Countries should use one or more of the following mechanisms to ensure that information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or can be otherwise determined in a timely manner by a competent authority:

a) requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;

b) requiring companies to take reasonable measures to obtain and hold up-to-date information on the companies' beneficial ownership;

c) using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with Recommendations 10 and 22; (ii) information held by other competent authorities on the legal and beneficial ownership of companies; (iii) information held by the company as required in criterion 24.3 above; and (iv) available information on companies listed on a stock exchange, where disclosure requirements ensure adequate transparency of beneficial ownership.

24.7. Countries should require that the beneficial ownership information is accurate and as upto-date as possible.

24.8. Countries should ensure that companies co-operate with competent authorities to the fullest extent possible in determining the beneficial owner, by:

a) requiring that one or more natural persons resident in the country is authorised by the company[123], and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

b) requiring that a DNFBP in the country is authorised by the company, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

c) taking other comparable measures, specifically identified by the country.

24.9. All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should be required to 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.

Other Requirements

24.10. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to obtain timely access to the basic and beneficial ownership information held by the relevant parties.

24.11. Countries that have legal persons able to issue bearer shares or bearer share warrants should apply one or more of the following mechanisms to ensure that they are not misused for money laundering or terrorist financing:

a) prohibiting bearer shares and share warrants; or

b) converting bearer shares and share warrants into registered shares or share warrants (for example through dematerialisation); or

c) immobilising bearer shares and share warrants by requiring them to be held with a regulated financial institution or professional intermediary; or

d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity; or

e) using other mechanisms identified by the country.

[123] Members of the company's board or senior management may not require specific authorisation by the company.

24.12. Countries that have legal persons able to have nominee shares and nominee directors should apply one or more of the following mechanisms to ensure they are not misused:

a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register;

b) requiring nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request; or

c) using other mechanisms identified by the country.

24.13. There should be liability and proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to comply with the requirements.

24.14. Countries should rapidly provide international co-operation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include:

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

b) exchanging information on shareholders; and

c) using their competent authorities' investigative powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts.

24.15. Countries should monitor 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.

INTERPRETIVE NOTE TO RECOMMENDATION 24 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS)

1. Competent authorities should be able to obtain, or have access in a timely fashion to, adequate, accurate and up-to-date information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information[124]) that are created[125] in the country, as well as those that present ML/TF risks and have sufficient links[126] with their country (if they are not created in the country). Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements set out below. Countries should utilise a combination of mechanisms to achieve the objective.

2. As part of the process described in paragraph 1 of ensuring that there is adequate transparency regarding legal persons, countries should have mechanisms that:

a) identify and describe the different types, forms and basic features of legal persons in the country.

b) identify and describe the processes for: (i) the creation of those legal persons; and (ii) the obtaining and recording of basic and beneficial ownership information;

c) make the above information publicly available;

---

[124] ***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%).

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

[126] 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.

d) assess the money laundering and terrorist financing risks associated with different types of legal persons created in the country, and take appropriate steps to manage and mitigate the risks that they identify; and

e) assess the money laundering and terrorist financing risks 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[127]

A. BASIC INFORMATION

3. In order to determine who the beneficial owners of a company[128] are, competent authorities will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors.

4. All companies created in a country should be registered in a company registry.[129] Whichever combination of mechanisms is used to obtain and record beneficial ownership information (see section B), there is a set of basic information on a company that needs to be obtained and recorded by the company[130] as a necessary prerequisite. The minimum basic information to be obtained and recorded by a company should be:

   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 or equivalent (where this exists);[131] and

   b) a register of its shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder[132] and categories of shares (including the nature of the associated voting rights).

5. The company registry[133] should record all the basic information set out in paragraph 4(a) above.

6. The company should maintain the basic information set out in paragraph 4(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.

B. BENEFICIAL OWNERSHIP INFORMATION

7. 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. 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. This should include the following:

   (a) Countries should require companies to obtain and hold adequate, accurate and up-to-date 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

---

[127] 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 paragraph 7.

[128] Recommendation 24 applies to all forms of legal persons. The requirements are described primarily with reference to companies, but similar requirements should be applied to other types of legal person, taking into account their different forms and structures - as set out in Section E.

[129] "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.

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

[131] This information should be made public, as set out in paragraph 11.

[132] This is applicable to the nominal owner of all registered shares.

[133] Or another public body in the case of a tax identification number.

financial institutions/DNFBPs to provide adequate, accurate and up-to-date information on the company's beneficial ownership information.

b) (i) Countries should require adequate, accurate and up-to-date information on the beneficial ownership of legal persons to be held by a public authority or body (for example a tax authority, FIU, company registry, or beneficial ownership registry). Information need not be held by a single body only.[134]

b) (ii) Countries may decide to use an alternative mechanism instead of (b)(i) if it also provides authorities with efficient access to adequate, accurate and up-to-date BO 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.

c) 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 obtained by financial institutions and/or DNFBPs in accordance with Recommendations 10 and 22.[135]

8. All the persons, authorities and entities mentioned above, 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.

C. TIMELY ACCESS TO ADEQUATE, ACCURATE AND UP-TO-DATE INFORMATION

9. 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 paragraph 7, is adequate, accurate and up to date.

Adequate information is information that is sufficient to identify[136] the natural person(s) who are the beneficial owner(s), and the means and mechanisms through which they exercise beneficial ownership or control.

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.

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.

10. 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 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.

---

[134] 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.

[135] 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.

[136] 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.

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 paragraph 4(a) above. Countries should also consider facilitating timely access by financial institutions and DNFBPs to information referred to in paragraph 4(b) above and to beneficial ownership information held pursuant to paragraph 7 above, and could consider facilitating public access to this information.

D. OBSTACLES TO TRANSPARENCY

12. Countries should take measures to prevent and mitigate the risk of the misuse of bearer shares and bearer share warrants[137] by prohibiting the issuance of new bearer shares and bearer share warrants; and, for any existing bearer shares and bearer share warrants, by applying one or more of the following mechanisms within a reasonable timeframe[138]:

    (a) converting them into a registered form; or

    (b) immobilising 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

    (c) during the period before (a) or (b) 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.

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 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 paragraph 7. Nominee status should be included in public information;

    (b) requiring nominee shareholders and directors to be licensed[139], 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 paragraph 7 and for them to maintain information identifying their nominator and the natural person on whose behalf the nominee is ultimately acting[140], and make this information available to the competent authorities upon request;[141] or

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

E. OTHER LEGAL PERSONS

14. In relation to foundations, Anstalt, Waqf[142] 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.

15. As regards other types of legal persons, countries should take into account the different forms and structures of those 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

---

[137] Or any other similar instruments without traceability.

[138] 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.

[139] 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.

[140] 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.

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

[142] Except in countries where Waqf are legal arrangements under R.25.

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. Countries should review the money laundering and terrorist financing risks associated with such other legal persons, and, based on the level of risk, determine the measures that should be taken to ensure that competent authorities have timely access to adequate, accurate and up-to-date beneficial ownership information for such legal persons.

F. LIABILITY AND SANCTIONS

16. There should be a clearly stated responsibility to comply with the requirements in this Interpretive Note, as well as liability and effective, proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to properly comply with the requirements.

G. INTERNATIONAL COOPERATION

17. 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. This should include (a) facilitating access by foreign competent authorities to basic information held by company registries; (b) exchanging information on shareholders; and (c) using their powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts. Countries should monitor 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. Consistent with Recommendations 37 and 40, countries should not place 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. Information held or obtained for the purpose of identifying beneficial ownership should be kept in a readily accessible manner in order to facilitate rapid, constructive and effective international co-operation. Countries should designate and make publicly known the agency(ies) responsible for responding to all international requests for BO information.

RECOMMENDATION 25	TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS[143]

Countries should assess the risks of the misuse of legal arrangements for money laundering or terrorist financing and take measures to prevent their misuse. In particular, countries should ensure that there is adequate, accurate and up-to-date information on express trusts and other similar legal arrangements including information on the settlor(s), trustee(s) and beneficiary(ies), that can be obtained or accessed efficiently and in a timely manner by competent authorities. Countries should consider facilitating access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

Main criteria

25.1. Countries should require:

a) trustees of any express trust governed under their law[144] to obtain and hold adequate, accurate, and current information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust;

b) trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors; and

c) professional trustees to maintain this information for at least five years after their involvement with the trust ceases.

25.2. Countries should require that any information held pursuant to this Recommendation is kept accurate and as up to date as possible, and is updated on a timely basis.

25.3. All countries should take measures to ensure that trustees disclose their status to financial institutions and DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold.

25.4. Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust[145]; or from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

25.5. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to information held by trustees, and other parties (in particular information held by financial institutions and DNFBPs), on the beneficial ownership and control of the trust, including: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets

[143] The measures required by Recommendation 25 are set out with specific reference to trusts. This should be understood as referring to express trusts (as defined in the glossary). In relation to other types of legal arrangement with a similar structure or function, countries should take similar measures to those required for trusts, with a view to achieving similar levels of transparency. At a minimum, countries should ensure that information similar to that specified in respect of trusts should be recorded and kept accurate and current, and that such information is accessible in a timely way by competent authorities. When considering examples provided in the Glossary definition of legal arrangement, assessors are reminded that the examples provided should not be considered definitive. Assessors should refer to the Glossary definition of trust and trustee which references Article 2 of the Hague Convention on the law applicable to trusts and their recognition when determining whether a legal arrangement has a similar structure or function to an express trust and therefore falls within the scope of R.25, regardless of whether the country denominates the legal arrangement using the same terminology. If a country does not apply the relevant obligations of R.25 on trustees (or those performing a similar function in relation to other legal arrangements), assessors should confirm whether such exemptions are consistent with criterion 1.6.

[144] Countries are not required to give legal recognition to trusts. Countries need not include the requirements of Criteria 25.1; 25.2; 25.3; and 25.4 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

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

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

25.6. Countries should rapidly provide international co-operation 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:

a) facilitating access by foreign competent authorities to basic information held by registries or other domestic authorities;

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

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

25.7. Countries should ensure that trustees are either (a) legally liable for any failure to perform the duties relevant to meeting their obligations; or (b) that there are proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply[146].

25.8. Countries should ensure that there are 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 criterion 25.1.

INTERPRETIVE NOTE TO RECOMMENDATION 25 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS)

1. Countries should require trustees of any express trust 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, to obtain and hold adequate, accurate, and up-to-date beneficial ownership information[147] 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[148] 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. Where the parties to the trusts or other similar legal arrangements are legal persons or arrangements, countries should require trustees and persons holding an equivalent position in a similar legal arrangement to also obtain and hold adequate, accurate, and up-to-date basic and beneficial ownership information of the legal persons or arrangements. Countries should also require trustees and persons holding an equivalent position in a similar legal arrangement that are residents in their country or that administer trusts or similar legal arrangements in their country 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.

[146] This does not affect the requirements for proportionate and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

[147] 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.

[148] 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.

2. Countries with express trusts and other similar legal arrangements governed under their law 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[149] and beneficial ownership information;

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

3. Countries should assess the money laundering and terrorist financing risks associated with different types of trusts and other similar legal arrangements:

   (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[150] with their country and take appropriate steps to manage and mitigate the risks that they identify.[151]

4. Countries should take measures to ensure that trustees or persons holding equivalent positions in similar legal arrangements 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. Trustees or persons holding equivalent positions in similar legal arrangements should cooperate to the fullest extent possible with, and not be prevented by law or enforceable means from providing competent authorities with necessary information relating to the trust or other similar legal arrangements.[152] Countries should also ensure that trustees or persons holding equivalent positions in similar legal arrangements should not be prevented by law or enforceable means from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust or legal arrangement to be held or managed under the terms of the business relationship.

5. In order to ensure that adequate, accurate and up-to-date information 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,

[149] 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.

[150] 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.

[151] 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.

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

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.[153]

(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.

6. Countries should have mechanisms that ensure that information on trusts and other similar legal arrangements, including information provided in accordance with paragraphs 4 and 5, is adequate, accurate and up-to-date.[154] In the context of legal arrangements:

- *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.[155]
- *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.
- *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.

7. 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.

8. Trustees and persons holding equivalent positions in similar legal arrangements should be required to maintain the information referred to in paragraph 1 for at least five years after their involvement with the trust or similar legal arrangement ceases. Countries are encouraged to require the other authorities, persons and entities mentioned in paragraph 5 above to maintain the information for at least five years.

9. Countries should require that any information held pursuant to paragraph 1 above should be kept accurate and up-to-date, and the information should be updated within a reasonable period following any change.

---

[153] 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.

[154] 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.

[155] 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.

10. Countries should consider measures to facilitate access to information that is held on trusts or other similar legal arrangements by the other authorities, persons and entities referred to in paragraph 5, by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

11. In the context of this Recommendation, countries are not required to give legal recognition to trusts. Countries need not include the requirements of paragraphs 1, 4, 8, 9 and 13 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

International Cooperation

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 (a) facilitating access by foreign competent authorities to any information held by registries or other domestic authorities; (b) exchanging domestically available information on the trusts or other legal arrangement; and (c) using their competent authorities' powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts. Consistent with Recommendations 37 and 40, countries should not place 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. To facilitate rapid, constructive and effective international cooperation, where possible, countries should designate and make 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.

Liability and Sanctions

13. Countries should ensure that there are clear responsibilities to comply with the requirements in this Interpretive Note; and that trustees or persons holding equivalent positions in similar legal arrangements are either legally liable for any failure to perform the duties relevant to meeting the obligations in paragraphs 1, 4, 8 and 9; or that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply.[156] Countries should ensure that 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 paragraphs 1 and 8.

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

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES

RECOMMENDATION 26	REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. 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. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

Main criteria

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[157], 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.

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:

[157] 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, 3-11, 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.

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.

INTERPRETIVE NOTE TO RECOMMENDATION 26 (REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS)

Risk-based approach to Supervision

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising institutions that apply an AML/CFT risk-based approach.

2. Adopting a risk-based approach to supervising financial institutions' AML/CFT systems and controls allows supervisory authorities to shift resources to those areas that are perceived to present higher risk. As a result, supervisory authorities can use their resources more effectively. This means that supervisors: (a) should have a clear understanding of the money laundering and terrorist financing risks present in a country; and (b) should have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised institutions, including the quality of the compliance function of the financial institution or group. The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions/groups should be based on the money laundering and terrorist financing risks, and the policies, internal controls and procedures associated with the institution/group, as identified by the supervisor's assessment of the institution/group's risk profile, and on the money laundering and terrorist financing risks present in the country.

3. The assessment of the money laundering and terrorist financing risk profile of a financial institution/group, including the risks of non-compliance, should be reviewed both periodically and when there are major events or developments in the management and operations of the financial institution/group, in accordance with the country's established practices for ongoing supervision. This assessment should not be static: it will change depending on how circumstances develop and how threats evolve.

4. AML/CFT supervision of financial institutions/groups that apply a risk-based approach should take into account the degree of discretion allowed under the RBA to the financial institution/group, and encompass, in an appropriate manner, a review of the risk assessments underlying this discretion, and of the adequacy and implementation of its policies, internal controls and procedures.

5. These principles should apply to all financial institutions/groups. To ensure effective AML/CFT supervision, supervisors should take into consideration the characteristics of the financial institutions/groups, in particular the diversity and number of financial institutions, and the degree of discretion allowed to them under the RBA.

Resources of supervisors

6. Countries should ensure that financial supervisors have adequate financial, human and technical resources. These supervisors should have sufficient operational independence and autonomy to ensure

freedom from undue influence or interference. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

RECOMMENDATION 27	POWERS OF SUPERVISORS

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

Main criteria

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

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

27.3. Supervisors should be authorised to compel[158] production of any information relevant to monitoring compliance with the AML/CFT requirements.

27.4. 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.

[158] 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

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:

- casinos should be licensed;
- 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, holding a management function in, or being an operator of, a casino; and
- competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) 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, e.g. through evaluating persons on the basis of a "fit and proper" test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

Main criteria

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.

INTERPRETIVE NOTE TO RECOMMENDATION 28 (REGULATION AND SUPERVISION OF DNFBPS)

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor or SRB, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising or monitoring DNFBPs that apply an AML/CFT risk-based approach.

2. Supervisors or SRBs should determine the frequency and intensity of their supervisory or monitoring actions on DNFBPs on the basis of their understanding of the money laundering and terrorist financing risks, and taking into consideration the characteristics of the DNFBPs, in particular their diversity and number, in order to ensure effective AML/CFT supervision or monitoring. This means having a clear understanding of the money laundering and terrorist financing risks: (a) present in the country; and (b) associated with the type of DNFBP and their customers, products and services.

3. Supervisors or SRBs assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs should properly take into account the money laundering and terrorist financing risk profile of those DNFBPs, and the degree of discretion allowed to them under the RBA.

4. Supervisors or SRBs should have adequate powers to perform their functions (including powers to monitor and sanction), and adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

OPERATIONAL AND LAW ENFORCEMENT

RECOMMENDATION 29	FINANCIAL INTELLIGENCE UNITS (FIUs)

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

Main criteria

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.[159]

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[160]:

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[161] 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

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;

---

[159] 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.

[160] 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").

[161] 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) 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.

INTERPRETIVE NOTE TO RECOMMENDATION 29 (FINANCIAL INTELLIGENCE UNITS)

A. GENERAL

1. This note explains the core mandate and functions of a financial intelligence unit (FIU) and provides further clarity on the obligations contained in the standard. The FIU is part of, and plays a central role in, a country's AML/CFT operational network, and provides support to the work of other competent authorities. 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.

B. FUNCTIONS

(a) Receipt

2. The FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

(b) Analysis

3. FIU analysis should add value to the information received and held by the FIU. While all the information should be considered, the analysis may focus either on each single disclosure received or on appropriate selected information, depending on the type and volume of the disclosures received, and on the expected use after dissemination. FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links. However, such tools cannot fully replace the human judgement element of analysis. FIUs should conduct the following types of analysis:

- Operational analysis uses available and obtainable information to identify specific targets (e.g. persons, assets, criminal networks and associations), 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 or terrorist financing.
- Strategic analysis 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. This information is then also used by the FIU or other state entities in order to determine money laundering and terrorist financing related threats and vulnerabilities. Strategic analysis may also help establish policies and goals for the FIU, or more broadly for other entities within the AML/CFT regime.

(c) Dissemination

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

- **Spontaneous dissemination**: The FIU should be able to disseminate information and the results of its analysis to competent authorities when there are grounds to suspect money laundering, predicate offences or terrorist financing. Based on the FIU's analysis, the dissemination of information should be selective and allow the recipient authorities to focus on relevant cases/information.
- **Dissemination upon request:** The FIU should be able to respond to information requests from competent authorities pursuant to Recommendation 31. When the FIU receives such a request from a competent authority, the decision on conducting analysis and/or dissemination of information to the requesting authority should remain with the FIU.

C. ACCESS TO INFORMATION

(a) Obtaining Additional Information from Reporting Entities

5. In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly. The information that the FIU should be permitted to obtain could include information that reporting entities are required to maintain pursuant to the relevant FATF Recommendations (Recommendations 10, 11 and 22).

(b) Access to Information from other sources

6. In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. 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.

D. INFORMATION SECURITY AND CONFIDENTIALITY

7. Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations. An FIU must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination, and protection of, as well as access to such information. The FIU should ensure that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. The FIU should ensure that there is limited access to its facilities and information, including information technology systems.

E. OPERATIONAL INDEPENDENCE

8. The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or disseminate specific information. In all cases, this means that the FIU has the independent right to forward or disseminate information to competent authorities.

9. An FIU may be established as part of an existing authority. When a FIU is located within the existing structure of another authority, the FIU's core functions should be distinct from those of the other authority.

10. The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively. Countries

should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

11. The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information.

F. UNDUE INFLUENCE OR INTERFERENCE

12. The FIU should be 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.

G. EGMONT GROUP

13. Countries should ensure that the FIU has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIUs). The FIU should apply for membership in the Egmont Group.

H. LARGE CASH TRANSACTION REPORTING

14. Countries should consider the feasibility and utility of a system where financial institutions and DNFBPs would report all domestic and international currency transactions above a fixed amount.

RECOMMENDATION 30	RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize criminal property and property of corresponding value. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place.

Main criteria

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[162], 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.

INTERPRETIVE NOTE TO RECOMMENDATION 30 (RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES)

1. There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation. Countries should also designate one or more competent authorities to identify, trace, and initiate freezing and seizing of criminal property and property of corresponding value.

2. A 'financial investigation' means an enquiry into the financial affairs related to criminal activity, with a view to:

   - identifying the extent of criminal networks and/or the scale of criminality;
   - identifying and tracing criminal property and property of corresponding value; and

[162] 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.

- developing evidence which can be used in criminal and/or confiscation proceedings.

3. 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). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations.

4. Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering and terrorist financing cases to postpone or waive the arrest of suspected persons and/or the seizure of the money, for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

5. 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.

6. Anti-corruption enforcement authorities with enforcement powers may be designated to investigate money laundering and terrorist financing offences arising from, or related to, corruption offences under Recommendation 30, and these authorities should also have sufficient powers to identify, trace, and initiate freezing and seizing of criminal property and property of corresponding value.

7. The range of law enforcement agencies and other competent authorities mentioned above should be taken into account when countries make use of multi-disciplinary groups in financial investigations.

8. Law enforcement authorities and prosecutorial authorities, including those authorities responsible for asset recovery, should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

RECOMMENDATION 31	POWERS OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities 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 the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence. Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery.

Countries should ensure that competent authorities have timely access to a wide range of information, particularly to support the identification and tracing of criminal property and property of corresponding value. This may include, but is not limited to, basic and beneficial ownership information, information held by tax authorities, information held in asset registries (such as for land, property, vehicles, shares, or other assets), and information held in citizenship, residency, or social benefit registries.

In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

Main criteria

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

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

Main criteria

Note to Assessors:

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 Annex I.

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 cooperation and assistance, in accordance with Recommendations 36 to 40. To facilitate such co-operation, information[163] 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.

INTERPRETIVE NOTE TO RECOMMENDATION 32 (CASH COURIERS)

A. OBJECTIVES

1. Recommendation 32 was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures to: (a) detect the physical crossborder transportation of currency and bearer negotiable instruments; (b) stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering; (c) stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed; (d) apply appropriate sanctions for making a false declaration or disclosure; and (e) enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering.

B. THE TYPES OF SYSTEMS THAT MAY BE IMPLEMENTED TO ADDRESS THE ISSUE OF CASH COURIERS

2. Countries may meet their obligations under Recommendation 32 and this Interpretive Note by implementing one of the following types of systems. However, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

Declaration system

3. All persons making a physical cross-border transportation of currency or bearer negotiable instruments (BNIs), which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system: (i) a written declaration system for all travellers; (ii) a written declaration system for those travellers carrying an amount of currency or BNIs above a threshold; and (iii) an oral declaration system. These three systems are described below in their pure form. However, it is not uncommon for countries to opt for a mixed system.

[163] 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).

a) *Written declaration system for all travellers*: In this system, all travellers are required to complete a written declaration before entering the country. This would include questions contained on common or customs declaration forms. In practice, travellers have to make a declaration whether or not they are carrying currency or BNIs (e.g. ticking a "yes" or "no" box).

b) *Written declaration system for travellers carrying amounts above a threshold:* In this system, all travellers carrying an amount of currency or BNIs above a pre-set designated threshold are required to complete a written declaration form. In practice, the traveller is not required to fill out any forms if they are not carrying currency or BNIs over the designated threshold.

c) *Oral declaration system for all travellers:* In this system, all travellers are required to orally declare if they carry an amount of currency or BNIs above a prescribed threshold. Usually, this is done at customs entry points by requiring travellers to choose between the "red channel" (goods to declare) and the "green channel" (nothing to declare). The choice of channel that the traveller makes is considered to be the oral declaration. In practice, travellers do not declare in writing, but are required to actively report to a customs official.

Disclosure system

4. Countries may opt for a system whereby travellers are required to provide the authorities with appropriate information upon request. In such systems, there is no requirement for travellers to make an upfront written or oral declaration. In practice, travellers need to be required to give a truthful answer to competent authorities upon request.

C. ADDITIONAL ELEMENTS APPLICABLE TO BOTH SYSTEMS

5. Whichever system is implemented, countries should ensure that their system incorporates the following elements:

a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and BNIs.

b) Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/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.

c) Information obtained through the declaration/disclosure process should be available to the FIU, either through a system whereby the FIU is notified about suspicious crossborder transportation incidents, or by making the declaration/disclosure information directly available to the FIU in some other way.

d) At the domestic level, countries should ensure that there is adequate coordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

e) In the following two cases, competent authorities should be able to stop or restrain cash or BNIs for a reasonable time, in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.

f) The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with Recommendations 36 to 40. To facilitate such cooperation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of USD/EUR 15,000 is made; or (ii) where there is a false declaration or false disclosure; or (iii) where there is a suspicion of money laundering or terrorist financing, this information shall be retained for use by competent authorities. At a minimum, this information will cover: (i) the amount of currency or BNIs declared, disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

g) Countries should implement Recommendation 32 subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

D. SANCTIONS

6. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or BNIs that is related to terrorist financing, money laundering or predicate offences should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, consistent with Recommendation 4, which would enable the confiscation of such currency or BNIs.

7. Authorities responsible for implementation of Recommendation 32 should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

E. GOLD, PRECIOUS METALS AND PRECIOUS STONES

8. For the purposes of Recommendation 32, gold, precious metals and precious stones are not included, despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action.

Glossary of specific terms used in this Recommendation

False declaration	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.
Physical cross-border transportation	refers to any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency or BNIs through containerised cargo or (3) the mailing of currency or BNIs by a natural or legal person.
Related to terrorist financing or money laundering	when used to describe currency or BNIs, refers to currency or BNIs that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money

	laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

GENERAL REQUIREMENTS

RECOMMENDATION 33	STATISTICS

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

Main criteria

33.1. Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems.[164] 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.

[164] For purposes of technical compliance, the assessment should be limited to the four areas listed below.

RECOMMENDATION 34	GUIDANCE AND FEEDBACK

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

Main criteria

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

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

Main criteria

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.[165]

35.2. Sanctions should be applicable not only to financial institutions and DNFBPs but also to their directors and senior management.

[165] 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.

G. INTERNATIONAL COOPERATION

RECOMMENDATION 36	INTERNATIONAL INSTRUMENTS

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

Main criteria

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[166] the Vienna Convention, the Palermo Convention, the Merida Convention[167] and the Terrorist Financing Convention.

[166] 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).

[167] 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

Countries should rapidly, constructively and effectively 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. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.

b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.

c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

d) Not refuse to execute a request for mutual legal assistance on the grounds that 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).

e) Maintain the confidentiality of mutual legal assistance requests 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. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

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.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and

b) a broad range of other powers and investigative techniques;

are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for

urgency, and should send requests using expeditious means. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

Main criteria

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

Countries should have measures, including legislative measures, to take expeditious action in response to requests by foreign countries seeking assistance to identify, trace, evaluate investigate, freeze, seize and confiscate criminal property and property of corresponding value. These measures should also enable countries to recognise and enforce foreign freezing, seizing, or confiscation orders. Further, countries should be able to manage property subject to confiscation at all stages of the asset recovery process and share or return confiscated property.

Countries should have in place the widest possible range of treaties, arrangements, or other mechanisms to enhance cooperation in asset recovery.

Main criteria

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.

INTERPRETIVE NOTE TO RECOMMENDATION 38 (MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION)

1. Countries should be able to take expeditious action in response to requests for cooperation in the widest possible range of circumstances. This should include requests made on the basis of conviction and non-conviction based confiscation proceedings and related provisional measures, as set out in Recommendation 4.[168]

2. In recognising and enforcing foreign freezing, seizing or confiscation orders, requested countries should be able to rely on the findings of fact in the foreign order. Enforcement should not be made conditional on conducting a domestic investigation. Further, courts in the requested country may review the foreign

[168] The reference to Recommendation 4 incorporates references to fundamental principles of domestic law which may relate to certain types of confiscation. With regard to requests made on the basis of non- conviction based confiscation proceedings, countries should have the authority to provide assistance, at a minimum, in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown, to the furthest extent that such assistance is consistent with fundamental principles of domestic law

order and issue any orders necessary to give it effect with regard to property located in the requested country.

3. Where the requested country requires a court order to provide assistance due to fundamental principles of domestic law or other considerations, requesting countries should ensure that their courts have authority to issue freezing, seizing, and confiscation orders for property located abroad or, if applicable, mechanisms for domestic judicial review and validation of orders to be submitted for enforcement.
4. Countries should also ensure they have the authority to provide further related assistance on an initial request, without requiring a supplemental request, in appropriate cases.
5. Countries should have effective mechanisms for managing, preserving, and, when necessary, disposing of, frozen, seized or confiscated property as set out in Recommendation 4.
6. Countries should be able to share confiscated property with other countries, in particular, when confiscation is directly or indirectly a result of coordinated law enforcement actions. Countries should be able to make arrangements, where appropriate, to deduct or share substantial or extraordinary costs incurred when enforcing a freezing, seizing, or confiscation order.
7. Countries should have measures to enable informal communication with other countries in asset recovery cases, including facilitating assistance before a request is made and updating countries, as appropriate, on the status of their requests.

RECOMMENDATION 39	EXTRADITION

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations. In particular, countries should:

a) ensure money laundering and terrorist financing are extraditable offences;

b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;

c) not place unreasonable or unduly restrictive conditions on the execution of requests; and

d) ensure they have an adequate legal framework for extradition.

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country 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. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

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.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, 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. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

Main criteria

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[169] in place.

[169] 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 COOPERATION

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.

Main criteria

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 cooperation 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[170].

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[171]

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.

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

[170] FIUs should be able to provide cooperation regardless of whether their counterpart FIU is administrative, law enforcement, judicial or other in nature.

[171] This refers to financial supervisors which are competent authorities and does not include financial supervisors which are SRBs.

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[172] 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.

INTERPRETIVE NOTE TO RECOMMENDATION 40 (OTHER FORMS OF INTERNATIONAL COOPERATION)

A. PRINCIPLES APPLICABLE TO ALL FORMS OF INTERNATIONAL COOPERATION

Obligations on requesting authorities

1. When making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable a timely and efficient execution of the request, as well as the foreseen use of the information requested. Upon request, requesting competent authorities should provide feedback to the requested competent authority on the use and usefulness of the information obtained.

Unduly restrictive measures

2. 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 (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; 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.

Safeguards on information exchanged

[172] 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.

3. Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorisation by the requested competent authority.

4. Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry[173], 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. Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in the manner authorised. Exchange of information should take place in a secure way, and through reliable channels or mechanisms. Requested competent authorities may, as appropriate, refuse to provide information if the requesting competent authority cannot protect the information effectively.

Power to search for information

5. Competent authorities should be able to conduct inquiries on behalf of a foreign counterpart, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

B. PRINCIPLES APPLICABLE TO SPECIFIC FORMS OF INTERNATIONAL COOPERATION

6. The general principles above should apply to all forms of exchange of information between counterparts or non-counterparts, subject to the paragraphs set out below.

Exchange of information between FIUs

7. FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, predicate offences and terrorist financing.

8. When making a request for cooperation, FIUs should make their best efforts to provide complete factual, and, as appropriate, legal information, including the description of the case being analysed and the potential link to the requested country. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

9. FIUs should have the power to exchange:

   a) all information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, 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.

10. Countries should ensure that the FIU or other competent authority is able to take immediate action, directly or indirectly, to withhold consent to or suspend a transaction suspected of being related to money laundering, predicate offences, or terrorist financing, in response to a relevant request from a foreign counterpart. If the competent authorities having this power in the requesting and the requested countries are not counterparts, countries should ensure that the FIU is able to send or receive such requests.

Exchange of information between financial supervisors[174]

11. Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. Efficient cooperation between financial supervisors aims at facilitating effective AML/CFT supervision of financial institutions. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent with the applicable international standards for supervision, in

[173] Information may be disclosed if such disclosure is required to carry out the request for cooperation.
[174] This refers to financial supervisors which are competent authorities.

particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

12. Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, and in a manner proportionate to their respective needs. Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other relevant 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 Principle Supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness.

    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.

13. 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.

14. Any dissemination of information exchanged or use of that information for supervisory and non-supervisory purposes, should be subject to prior authorisation by the requested financial supervisor, 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. The prior authorisation includes any deemed prior authorisation under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding issued by a core principles standard-setter applied to information exchanged under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding.

Exchange of information between law enforcement authorities

15. 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.

16. 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 cooperation, 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.

17. Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or multilateral arrangements to enable such joint investigations. Countries are encouraged to join and support existing AML/CFT law enforcement networks, and develop bi-lateral contacts with foreign law enforcement agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation.

18. Law enforcement authorities should be able to exchange domestically available information for intelligence or investigative purposes and cooperate with foreign counterparts to identify and trace criminal property and property of corresponding value, and in support of the freezing, seizing, and confiscation of such property through the formal mutual legal assistance process. Law enforcement authorities should be able to commence domestic investigations or proceedings based on such information received from foreign counterparts, in appropriate cases.

19. Law enforcement authorities should be able to spontaneously share relevant information regarding criminal property and property of corresponding value with foreign counterparts without a prior request, in appropriate cases. In addition, in appropriate cases, law enforcement authorities should be able to

spontaneously identify and trace criminal property and property of corresponding value if they suspect that such property relating to a foreign investigation may be located in their jurisdiction. Law enforcement authorities have discretion on when and under what conditions to share such information, for example, so as not to prejudice domestic investigations.

20. Countries should take part in and actively support multilateral networks to better facilitate rapid and constructive international cooperation in asset recovery. Countries should apply for membership in a relevant Asset Recovery Inter-agency Network (ARIN) or other body supporting international cooperation in asset recovery.

Exchange of information between non-counterparts

21. Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. 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. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

22. Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts.

METHOTOLOGY OF EFFECTIVENESS ASSESSMENT

Immediate Outcome 1	**Money laundering and terrorist financing risks are understood and, where appropriate, actions co-ordinated domestically to combat money laundering and the financing of terrorism and proliferation.**

Characteristics of an effective system

A country properly identifies, assesses and understands its money laundering and terrorist financing risks, and co-ordinates domestically to put in place actions to mitigate these risks. This includes the involvement of competent authorities and other relevant authorities; using a wide range of reliable information sources; using the assessment(s) of risks as a basis for developing and prioritising AML/CFT policies and activities; and communicating and implementing those policies and activities in a co-ordinated way across appropriate channels. The relevant competent authorities also co-operate, and co-ordinate policies and activities to combat the financing of proliferation. 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 also elements of R.15.

Note to Assessors:

1. Assessors are not expected to conduct an in-depth review of, or assess the country's assessment(s) of risks. Assessors, based on their views of the reasonableness of the assessment(s) of risks, should focus on how well the competent authorities use their understanding of the risks in practice to inform policy development and actions to mitigate the risks.
2. Assessors should take into consideration their findings for this Immediate Outcome (IO) in their assessment of the other IOs. However, assessors should only let their findings relating to the cooperation and co-ordination of measures to combat the financing of proliferation affect the assessments of IO.11 and not of the other IOs. (i.e. IO.2 to IO.10) that deal with combating money laundering and terrorist financing.

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

1.1. How well does the country understand its ML/TF risks?

1.2. How well are the identified ML/TF risks addressed by national AML/CFT policies and activities?

1.3. To what extent are the results of the assessment(s) of 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[175] and activities to combat ML/TF and, where appropriate, the financing of proliferation of weapons of mass destruction?[176]

1.6. To what extent does the country ensure that respective financial institutions, DNFBPs and other sectors affected by the application of the FATF Standards are aware of the relevant results of the national ML/TF risk assessment(s)?

---

[175] Having regard to AML/CFT requirements and Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation) as needed.

[176] Considering that there are different forms of co-operation and co-ordination between relevant authorities, Core Issue 1.5 does not prejudge a country's choice for a particular form and applies equally to all of them.

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. Outreach activities to private sector and relevant authorities (e.g., *briefings and guidance on relevant conclusions from risk assessment(s); frequency and relevancy of consultation on policies and legislation, input to develop risk assessment(s) and other policy products*).

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?
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? 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 mechanism(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 both policymaking and operational levels (and where relevant, the financing of proliferation of weapons of mass destruction)? Does the mechanism or body include all relevant authorities?
11. Is interagency information sharing undertaken in a timely manner on a bilateral or multiagency basis as appropriate?
12. Are there adequate resources and expertise involved in conducting the assessment(s) of risks, and for domestic co-operation and co-ordination?

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:

Assessors should take into consideration how their findings on the specific role of relevant competent authorities in seeking and delivering international co-operation under this IO would impact other IOs (particularly IO.3, IO.5, IOs. 6 to 10) including how the country seeks international co-operation with respect to domestic cases when appropriate.

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 across the range of international co-operation requests? What is the quality of such assistance provided?

2.2. To what extent has the country sought legal assistance for international co-operation in an appropriate and timely manner to pursue domestic ML, associated predicate offences and TF cases which have transnational elements?

2.3. To what extent do the different competent authorities seek other forms of international cooperation to exchange financial intelligence and supervisory, law enforcement or other information in an appropriate and timely manner with their foreign counterparts for AML/CFT purposes?

2.4. To what extent do the different competent authorities provide (including spontaneously) other forms of international co-operation to exchange financial intelligence and supervisory, law enforcement or other information in a constructive and timely manner with their foreign counterparts for AML/CFT purposes?

2.5. How well are the competent authorities providing and responding to foreign requests for cooperation in identifying and exchanging basic and beneficial ownership information of legal persons and arrangements?

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, or other co-operation mechanisms).
3. Examples of: (a) making requests for, and (b) providing successful 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 cooperation; value of assets repatriated or shared*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

5. 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?
6. What mechanisms (including case management systems) are used among the different competent authorities to receive, assess, prioritise and respond to requests for assistance?
7. What are the reasons for refusal in cases where assistance is not or cannot be provided?
8. What mechanisms (including case management systems) are used among the different competent authorities to select, prioritise and make requests for assistance?
9. 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?
10. 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?
11. 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?
12. To what extent does the country prosecute its own nationals without undue delay in situations when it is unable by law to extradite them?
13. What measures and arrangements are in place to manage and repatriate assets confiscated at the request of other countries?
14. Are there aspects of the legal, operational or judicial process (e.g., excessively strict application of dual criminality requirements etc.) that impede or hinder international cooperation?
15. To what extent are competent authorities exchanging information, indirectly, with non-counterparts?
16. Are adequate resources available 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	**Supervisors appropriately supervise, monitor and regulate financial institutions, DNFBPs and VASPs for compliance with AML/CFT requirements commensurate with their risks**

Characteristics of an effective system

Supervision and monitoring address and mitigate the money laundering and terrorist financing risks in the financial and other relevant 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, DNFBPs or VASPs; and
- promptly identifying, remedying, and sanctioning, where appropriate, violations of AML/CFT requirements or failings in money laundering and terrorist financing risk management.

Supervisors[177] provide financial institutions, DNFBPs and VASPs with adequate feedback and guidance on compliance with AML/CFT requirements. Over time, supervision and monitoring improve the level of AML/CFT compliance, and discourage attempts by criminals to abuse the financial, DNFBP and VASP sectors, particularly in the sectors most exposed to money laundering and terrorist financing risks.

This outcome relates primarily to Recommendations 14, 15, 26 to 28, 34 and 35, and also elements of Recommendations 1 and 40.

Note to Assessors:

1. Assessors should determine which financial, DNFBP and VASP sectors to weight as being most important, moderately important or less important, and should reflect their judgment in Chapters 1, 5 and 6 of the report. While judging on the overall effectiveness of this IO, assessors should explain how they have weighted the identified deficiencies and also explain how these have been taken into account in relation to how the assessors have weighted the different sectors.
2. When determining how to weight the various financial, DNFBP and VASP sectors, assessors should consider their relative importance, taking into account the following factors:
   a) the ML/TF risks facing each sector, taking into account the materiality relevant to each sector (e.g. the relative importance of different parts of the financial sector and different DNFBPs and VASPs; the size, integration and make-up of the financial sector[178]; 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), and
   b) structural elements and other contextual factors (e.g. whether established supervisors with accountability, integrity and transparency are in place for each sector; and the maturity and sophistication of the regulatory and supervisory regime for each sector)[179].

For more information on how assessors should take risk, materiality, structural elements and other contextual factors into account, see paragraphs 5 to 12 of the Methodology. For more guidance on how to reflect in the report their judgment on the relative importance of the financial, DNFBP and VASP sectors, see the Mutual Evaluation Report Template in Annex II of the Methodology.

[177] In relation to financial institutions and DNFBPs (but not to VASPs), references to "Supervisors" include SRBs for the purpose of the effectiveness assessment.

[178] E.g. including, but not limited to, the business concentration in the different sectors.

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

3. Assessors should also consider the relevant findings (including at the financial group level) on the level of international co-operation which supervisors are participating in when assessing this IO.

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, DNFBPs or VASPs? How well are breaches of such licensing or registration requirements detected?

3.2. How well do the supervisors identify and maintain an understanding of the ML/TF risks in the financial and other sectors as a whole, between different sectors and types of institution, and of individual institutions?

3.3. With a view to mitigating the risks, how well do supervisors, on a risk-sensitive basis, supervise or monitor the extent to which financial institutions, DNFBPs and VASPs are complying with their AML/CFT requirements?

3.4. To what extent are remedial actions and/or effective, proportionate and dissuasive sanctions applied in practice?

3.5. To what extent are supervisors able to demonstrate that their actions have an effect on compliance by financial institutions, DNFBPs and VASPs?

3.6. How well do the supervisors promote a clear understanding by financial institutions, DNFBPs and VASPs of their AML/CFT obligations and ML/TF risks?

a) Examples of Information that could support the conclusions on Core Issues

1. Contextual factors regarding the size, composition, and structure of the financial, DNFBP and VASP sectors and informal or unregulated sector (e.g., *number and types of financial institutions (including MVTS), DNFBPs and VASPs licensed or registered in each category; types of financial (including cross-border) activities; relative size, importance and materiality of sectors*).
2. Supervisors' risk 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 practises, thematic studies; annual reports*).
3. Information on supervisory engagement with the industry, the FIU and other competent authorities on AML/CFT issues (e.g., *providing guidance and training, organising meetings or promoting interactions with financial institutions, DNFBPs and VASPs*).
4. Information on supervision (e.g., *frequency, scope and nature of monitoring and inspections (on-site and off-site); nature of breaches identified; sanctions and other remedial actions* (e.g., *corrective actions, reprimands, fines) applied, examples of cases where sanctions and other remedial actions have improved AML/CFT compliance*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

5. What are the measures implemented to prevent the establishment or continued operation of shell banks in the country?
6. 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, DNFBPs and VASPs?
7. 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)?
8. What measures and supervisory tools are employed to ensure that financial institutions (including financial groups), DNFBPs and VASPs are regulated and comply with their AML/CFT obligations (including those which relate to targeted financial sanctions on terrorism, and to countermeasures called for by the FATF)? To what extent has this promoted the use of the formal financial system?

9. 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), DNFBPs and VASPs?
10. What is the level of co-operation between supervisors and other competent authorities in relation to AML/CFT (including financial group ML/TF risk management) issues? What are the circumstances where supervisors share or seek information from other competent authorities with regard to AML/CFT issues (including market entry)?
11. 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?
12. 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?
13. 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?

Immediate Outcome 4	**Financial institutions, DNFBPs and VASPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.**

Characteristics of an effective system

Financial institutions, DNFBPs and VASPs understand the nature and level of their money laundering and terrorist financing risks; develop and apply AML/CFT policies (including groupwide 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 to 23, and also elements of Recommendations 1, 6 and 29.

Note to Assessors:

1. Assessors should determine which financial, DNFBP and VASP sectors to weight as being most important, moderately important or less important, and should reflect their judgment in Chapters 1, 5 and 6 of the report. While judging on the overall effectiveness of this IO, assessors should explain how they have weighted the identified deficiencies and also explain how these have been taken into account in relation to how the assessors have weighted the different sectors.
2. When determining how to weight the various financial, DNFBP and VASP sectors, assessors should consider their relative importance, taking into account the following factors:
   a) the ML/TF risks facing each sector, taking into account the materiality relevant to each sector (e.g. the relative importance of different parts of the financial sector and different DNFBPs and VASPs; the size, integration and make-up of the financial sector[180]; 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), and
   b) structural elements and other contextual factors (e.g. whether established supervisors with accountability, integrity and transparency are in place for each sector; and the maturity and sophistication of the regulatory and supervisory regime for each sector).[181]

For more information on how assessors should take risk, materiality, structural elements and other contextual factors into account, see paragraphs 5 to 12 of the Methodology. For more guidance on how to reflect in the report their judgment on the relative importance of the financial, DNFBP and VASP sectors, see the Mutual Evaluation Report Template in Annex II of the Methodology.

3. Assessors are not expected to conduct an in-depth review of the operations of financial institutions, DNFBPs or VASPS, but should consider, on the basis of evidence and interviews with supervisors, FIUs, financial institutions, DNFBPs and VASPs, 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 these risks; and whether regulatory requirements (including STR reporting) are being properly implemented.

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

[180] E.g. including, but not limited to, the business concentration in the different sectors.
[181] E.g. special supervisory activities, such as thematic reviews and targeted outreach to specific sectors or institutions.

4.1. How well do financial institutions, DNFBPs and VASPs understand their ML/TF risks and AML/CFT obligations?

4.2. How well do financial institutions, DNFBPs and VASPs apply mitigating measures commensurate with their risks?

4.3. How well do financial institutions, DNFBPs and VASPs apply the CDD and record-keeping measures (including beneficial ownership information and ongoing monitoring)? To what extent is business refused when CDD is incomplete?

4.4. How well do financial institutions, DNFBPs and VASPs apply the enhanced or specific measures for: (a) PEPs, (b) correspondent banking, (c) new technologies, (d) wire transfer rules[182], (e) targeted financial sanctions relating to TF, and (f) higher-risk countries identified by the FATF?

4.5. To what extent do financial institutions, DNFBPs and VASPs meet their reporting obligations on the suspected proceeds of crime and funds in support of terrorism? What are the practical measures to prevent tipping-off?

4.6. How well do financial institutions, DNFBPs and VASPs apply internal controls and procedures (including at financial group level) to ensure compliance with AML/CFT requirements? To what extent are there legal or regulatory requirements (e.g., financial secrecy) impeding its implementation?

a) Examples of Information that could support the conclusions on Core Issues

1. Contextual factors regarding the size, composition, and structure of the financial, DNFBP and VASP sectors and informal or unregulated sector (e.g., *number and types of financial institutions (including MVTS), DNFBPs and VASPs licensed or registered in each category; types of financial (including cross-border) activities; relative size, importance and materiality of sectors*).
2. Information (including trends) relating to risks and general levels of compliance (e.g., *internal AML/CFT policies, procedures and programmes, trends and typologies reports*).
3. Examples of compliance failures (e.g., *sanitised cases; typologies on the misuse of financial institutions, DNFBPs and VASPs*).
4. Information on compliance by financial institutions, DNFBPs and VASPs (e.g., *frequency of internal AML/CFT compliance review; nature of breaches identified and remedial actions taken or sanctions applied; 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*).
5. Information on STR reporting and other information as required by national legislation (e.g., *number 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; average time taken to analyse the suspicious transaction before filing an STR*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

6. What are the measures in place to identify and deal with higher (and where relevant, lower) risk customers, business relationships, transactions, products and countries?
7. Does the manner in which AML/CFT measures are applied prevent the legitimate use of the formal financial system, and what measures are taken to promote financial inclusion?
8. 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? What is the relative level of compliance between international financial groups and domestic institutions?
9. To what extent is there reliance on third parties for the CDD process and how well are the controls applied?

[182] In the context of VASPs, this refers to virtual asset transfer rules.

10. How well do financial institutions and groups, DNFBPs and VASPs ensure adequate access to information by the AML/CFT compliance function?
11. Do internal policies and controls of the financial institutions and groups, DNFBPs and VASPs 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?
12. What are the measures and tools employed to assess risk, formulate and review policy responses, and institute appropriate risk mitigation and systems and controls for ML/TF risks?
13. How are AML/CFT policies and controls communicated to senior management and staff? What remedial actions and sanctions are taken by financial institutions, DNFBPs and VASPs when AML/CFT obligations are breached?
14. How well are financial institutions, DNFBPs and VASPs documenting their ML/TF risk assessments, and keeping them up to date?
15. Do financial institutions, DNFBPs and VASPs have adequate resources to implement AML/CFT policies and controls relative to their size, complexity, business activities and risk profile?
16. How well is feedback provided to assist financial institutions, DNFBPs and VASPs 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

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 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, 37 and 40.

Note to Assessors:

Assessors should also consider the relevant findings in relation to the level of international cooperation 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.

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

5.1. To what extent is the information on the creation and types of legal persons and arrangements in the country available publicly?

5.2. How well do the relevant competent authorities identify, assess and understand the vulnerabilities, and the extent to which legal persons created in the country can be, or are being misused for ML/TF?

5.3. How well has the country implemented measures to prevent the misuse of legal persons and arrangements for ML/TF purposes?

5.4. To what extent can relevant competent authorities obtain adequate, accurate and current basic and beneficial ownership information on all types of legal persons created in the country, in a timely manner?

5.5. To what extent can relevant competent authorities obtain adequate, accurate and current beneficial ownership information on legal arrangements, in a timely manner?

5.6. 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.
2. Experiences of law enforcement and other relevant competent authorities (e.g., *level of sanctions imposed for breach of the information requirements; where and how basic and beneficial ownership information (including information on the settlor, trustee(s), protector and beneficiaries) is obtained; information used in supporting investigation*).

3. Typologies and examples of the misuse of legal persons and arrangements (e.g., *frequency with which criminal investigations find evidence of the country's legal persons and arrangements being used for ML/TF; legal persons misused for illegal activities dismantled or struck-off).*
4. 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*).
5. 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.
6. Other information (e.g., *information on existence of legal arrangements; responses (positive and negative) to requests for basic or beneficial ownership information received from other countries; information on the monitoring of quality of assistance*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

7. What are the measures taken to enhance the transparency of legal persons (including dealing with bearer shares and share warrants, and nominee shareholders and directors) and arrangements?
8. How do relevant authorities ensure that accurate and up-to-date basic and beneficial ownership information on legal persons is maintained? Is the presence and accuracy of information monitored, tested/certified or verified?
9. To what extent is the time taken for legal persons to register changes to the required basic and beneficial ownership information adequate to ensure that the information is accurate and up to date? Where applicable, to what extent are similar changes in legal arrangements registered in a timely manner?
10. To what extent can financial institutions and DNFBPs obtain accurate and up-to-date basic and beneficial ownership information on legal persons and arrangements? What is the extent of information that trustees disclose to financial institutions and DNFBPs?
11. Do the relevant authorities have adequate resources to implement the measures adequately?

Immediate Outcome 6	**Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.**

Characteristics of an effective system

A wide variety of financial intelligence and other relevant information is collected and used by competent authorities to investigate money laundering, associated predicate offences and terrorist financing. This delivers reliable, accurate, and up-to-date information; and the competent authorities have the resources and skills to use the information to conduct their analysis and financial investigations, to identify and trace the assets, and to develop operational analysis.

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. This outcome includes the work that the FIU does to analyse STRs and other data; and the use by competent authorities of FIU products, other types of financial intelligence and other relevant information[183].
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 FIUs and law enforcement agencies are able to, and do seek appropriate financial and law enforcement intelligence and other information from their foreign counterparts.

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

6.1. To what extent are financial intelligence and other relevant information accessed and used in investigations to develop evidence and trace criminal proceeds related to ML, associated predicate offences and TF?

6.2. To what extent are the competent authorities receiving or requesting reports (e.g., STRs, reports on currency and bearer negotiable instruments) that contain relevant and accurate information that assists them to perform their duties?

6.3. To what extent is FIU analysis and dissemination supporting the operational needs of competent authorities?

6.4. To what extent do the FIU and other competent authorities co-operate and exchange information and financial intelligence? How securely do the FIU and competent authorities protect the confidentiality of the information they exchange or use?

a) Examples of Information that could support the conclusions on Core Issues

1. 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).*
2. 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*

[183] The sources include information derived from STRs, cross-border reports 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, benefits agencies, NPOs authorities; and information which can be obtained through compulsory measures from financial institutions and DNFBPs including CDD information and transaction records, as well as information from open sources.

intelligence was used in investigation and prosecution of ML/TF and associated predicate offences, or in identifying and tracing assets).

3. 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).*
4. 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).*
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 does the FIU ensure the rigour of its analytical assessments?
7. How well do competent authorities make use of the information contained in STRs and other financial intelligence to develop operational analysis?
8. To what extent does the FIU incorporate feedback from competent authorities, typologies and operational experience into its functions?
9. What are the mechanisms 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?
10. To what extent do the STRs reported contain complete, accurate and adequate information relating to the suspicious transaction?
11. To what extent do the relevant competent authorities review and engage (including outreach by the FIU) reporting entities to enhance financial intelligence reporting?
12. Do the relevant authorities have adequate resources (including IT tools for data mining and analysis of financial intelligence and to protect its confidentiality) to perform its functions?
13. What are the measures implemented to ensure that the FIU has operational independence so that it is not 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:

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.

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

7.1. How well, and in what circumstances are potential cases of ML identified and investigated (including through parallel financial investigations)?

7.2. To what extent are the types of ML activity being investigated and prosecuted consistent with the country's threats and risk profile and national AML/CFT policies?

7.3. To what extent are different types of ML cases prosecuted (*e.g.*, foreign predicate offence, third-party laundering, stand-alone offence[184] etc.) and offenders convicted?

7.4. To what extent are the sanctions applied against natural or legal persons convicted of ML offences effective, proportionate and dissuasive?

7.5. 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 investigations, prosecutions and convictions*(* e.g., *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 successful cases against domestic and transnational organised crime; cases where other criminal sanctions or measures are pursued instead of ML convictions).*

[184] **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** 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 the predicate offence. The proceeds may have been laundered by the defendant (self-laundering) or by a third party (third party ML).

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 imposed for ML offences; sanctions imposed for ML compared with those for other predicate offences).*

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:

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 confiscating[185] (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).*

[185] For the purposes of assessing the effectiveness of IO.8, full credit should be given for relevant use of the tax system, namely amounts recovered using tax assessment procedures that relate to the proceeds and instrumentalities of crime. The assessed country should ensure that any data provided is limited to tax recoveries that are linked to criminal proceeds/instrumentalities, or the figures should be appropriately caveated.

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 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.
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 cross-border terrorist financing cases.

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

9.1. To what extent are the different types of TF activity (*e.g.,* collection, movement and use of funds or other assets) prosecuted and offenders convicted? Is this consistent with the country's TF risk profile?

9.2. How well are cases of TF identified, and investigated? To what extent do the investigations identify the specific role played by the terrorist financier?

9.3. To what extent is the investigation of TF integrated with, and used to support, national counter-terrorism strategies and investigations (e.g., identification and designation of terrorists, terrorist organisations and terrorist support networks)?

9.4. To what extent are the sanctions or measures applied against natural and legal persons convicted of TF offences effective, proportionate and dissuasive?

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?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences and examples of TF investigations and prosecutions (e.g., *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).*
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 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, and from abusing the NPO sector.**

Characteristics of an effective system

Terrorists, terrorist organisations and terrorist support networks 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 regional sanctions regimes. The country also has a good understanding of the terrorist financing risks and takes appropriate and proportionate actions to mitigate those risks, including measures that prevent the raising and moving of funds through entities or methods which are at greatest risk of being misused by terrorists. 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, 30 to 32, 37, 38 and 40.

Note to Assessors:

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 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, without disrupting or discouraging legitimate NPO activities, has the country applied focused and proportionate measures to such NPOs which the country has identified as being vulnerable to terrorist financing abuse, in line with the risk-based approach?

10.3. To what extent are terrorists, terrorist organisations and terrorist financiers deprived (whether through criminal, civil or administrative processes) of assets and instrumentalities related to TF activities?

10.4. To what extent are the above measures consistent with the overall TF risk profile?

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 and confiscation (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 UNSCR1373); 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 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 (e.g., UNSCR 1452 and any successor resolutions)?
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 are all four of the following elements being used to identify, prevent and combat terrorist financing abuse of NPOs: (a) sustained outreach, (b) targeted risk-based supervision or monitoring, (c) effective investigation and information gathering, and (d) effective mechanisms for international cooperation. To what extent are the measures being applied focused and proportionate and in line with the risk-based approach such that NPOs are protected from terrorist financing abuse and legitimate charitable activities are not disrupted or discouraged?
11. To what extent are appropriate investigative, criminal, civil or administrative actions, cooperation and coordination 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/supervision/monitoring /investigation duties effectively?
12. How well do NPOs understand their vulnerabilities and comply with the measures to protect themselves from the threat of terrorist abuse?
13. Are there other aspects of the investigative, prosecutorial or judicial process that promote or hinder the identification, tracing and deprivation of assets and instrumentalities related to terrorists, terrorist organisations or terrorist financiers?
14. Do the relevant competent authorities have adequate resources to manage their work or address the terrorist financing risks adequately?
15. 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 and there is adequate co-operation and co-ordination between the relevant authorities to prevent sanctions from being evaded, and to develop and implement policies and activities to combat the financing of proliferation of WMD.

This outcome relates to Recommendation 7 and elements of Recommendations 2 and 15.

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

11.1. How well is the country implementing, without delay, targeted financial sanctions concerning the UNSCRs relating to the combating of financing of proliferation?

11.2. 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?

11.3. To what extent do financial institutions, DNFBPs and VASPs comply with, and understand their obligations regarding targeted financial sanctions relating to financing of proliferation?

11.4. 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. Monitoring and other relevant information 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

4. 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?
5. 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?

6. 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?
7. What mechanisms are used to prevent the evasion of sanctions? Do relevant competent authorities provide financial institutions, DNFBPs and VASPs with other guidance or specific feedback?
8. 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?
9. To what extent are the relevant competent authorities exchanging intelligence and other information for investigations of violations and breaches of targeted financial sanctions in relation to financing of proliferation, as per the relevant UNSCRs?
10. Do the relevant competent authorities have adequate resources to manage their work or address the financing of proliferation risks adequately?

ANNEX II
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 2013 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 is expected to be 100 pages or less (together with a technical 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. Nevertheless, assessors should ensure the MER does not become excessively long, and should be prepared to edit their analysis as necessary. In order 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 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.

ANNEX III

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 para. 29.

Guidance	Relevant FATF Standards/Methodology
National money laundering and terrorist financing risk assessment (05 Mar 2013) Terrorist Financing Risk Assessment Guidance (05 Jul 2019)	**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 (07 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 (19 Oct 2012)	**R.4** (Confiscation and Provisional Measures) **R.38** (Freezing and Confiscation)
Guidance on Criminalising Terrorist Financing (21 Oct 2016)	**R.5** (Terrorist Financing Offence)
International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6) (28 June 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 (28 Feb 2018)	**R.7** (Targeted Financial Sanctions related to Proliferation)
Best Practices on Combating the Abuse of Non-Profit Organisations (26 Jun 2015)	**R.8** (Non-Profit Organisations (NPOs))
Guidance on Digital ID (6 March 2020)	**R.10** (Customer due diligence (CDD)=
FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22) (27 Jun 2013)	**R.12** (Politically Exposed Persons (PEPs)) **R.22** (Designated Non-Financial Businesses and Professions (DNFBPs): Customer Due Diligence)

Guidance	Relevant FATF Standards/Methodology
Guidance on Correspondent Banking Services (21 Oct 2016)	**R.13** (Correspondent Banking)
Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (21 Jun 2019)	**R.15** (New technologies)
FATF Guidance - Private Sector Information Sharing (04 Nov 2017)	**R.18** (Internal Controls and Foreign Branches and Subsidiaries) **R.21** (Tipping-Off and Confidentiality)
Best Practices on Beneficial Ownership for Legal Persons (16 October 2019) Guidance on Transparency and Beneficial Ownership (27 Oct 2014)	**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)
Operational Issues - Financial Investigations Guidance (11 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 (27 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 (23 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 (04 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 Recommendations to Combat Corruption (18 Oct 2013)	**Methodology** *Introduction* (Corruption)

Guidance	Relevant FATF Standards/Methodology
• Guidance for a Risk Based Approach for Legal Professionals (26 Jun 2019) • Guidance for a Risk-Based Approach for the Accounting Profession (26 Jun 2019) • Guidance for a Risk-Based Approach for Trust and Company Service Providers (26 Jun 2019) • Guidance for a Risk-Based Approach: Life Insurance Sector (29 Oct 2018) • Guidance for a Risk-Based Approach: Securities Sector (29 Oct 2018) • Guidance for a Risk-Based Approach: Money or Value Transfer Services (23 Feb 2016) • Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement (23 Oct 2015) • Guidance for a Risk-Based Approach: Virtual Currencies (26 June 2015) • Guidance for a Risk-Based Approach: The Banking Sector (27 Oct 2014) • Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services (26 June 2013)	**Methodology** *Introduction* (RBA)

RULES OF PROCEDURE

FOR THE 5TH ROUND OF MUTUAL EVALUATIONS BY MONEYVAL[186]

The Committee of Experts on the evaluation of anti-money laundering measures and the financing of terrorism (hereinafter referred to as "MONEYVAL"),

Having regards to the Resolution CM/Res(2013)13 adopted by the Committee of Ministers of the Council of Europe on the Statute of the Committee of Experts on the evaluation of anti-money laundering measures and the financing of terrorism,

Pursuant to paragraph 1 of Article 5 of its Statute,

Adopts the following Rules of Procedure,

TITLE I. ORGANISATION OF MONEYVAL

Rule 1 – Composition of MONEYVAL

1. MONEYVAL shall consist of delegations and representatives of observer States, organisations, institutions or bodies, designated according to articles 3 and respectively 4 of MONEYVAL's statute. Each delegation shall appoint a Head of Delegation.

2. Countries and territories[187] subject to MONEYVVAL's evaluation processes shall promptly notify the Executive Secretary of any change in the composition of their delegation, and in particular as regards any change of the Head of Delegation. In the absence of such a notification, communications shall be addressed to the Permanent Representation of the relevant State to the Council of Europe.

Rule 2 – Other Representatives not Having the Right to Vote

1. Representatives appointed under article 4 of the Statute shall be entitled, upon the Chair's invitation, to make oral or written statements on the subjects under discussion.

Rule 3 – Functions of the Chair, Vice-Chairs and Bureau Members

1. The Chair shall preside over the plenary meetings, the meetings of the Bureau and any other relevant meetings and perform all functions conferred upon him or her by the Statute, by the Rules of procedure and by a decision of MONEYVAL.
2. The Chair may delegate certain of his or her functions to the Vice-Chairs, or, in their absence, to 1 or more of the members of the Bureau, or to the Executive Secretary.
3. The Vice-Chair who has served the longest on the Bureau shall take the place of the Chair if the latter is unable to carry out his or her duties. If both Vice-Chairs have served on the Bureau for the same period, they should decide who replaces the Chair, in consultation with the Executive Secretary.

[186] Adopted by MONEYVAL at its 46th Plenary meeting (Strasbourg, 8-12 December 2014), last revised through written procedure in the 4th Intersessional Consultation (Strasbourg, October 2021).

[187] The term "country or territory" in this document shall refer to the States covered under Article 2(2) of CM/Res(2013)3 on the Statute of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL); Israel (CM/Dec(2006)953/10.1E); the Holy See, including the Vatican City State (CM/Res(2011)5), the Crown Dependencies of Guernsey, Jersey and the Isle of Man (CM/Res(2012)6), and Gibraltar (CM/Res(2015)26) .

4. In the exercise of their duties, the Chair, the Vice-Chairs and the Bureau members shall undertake to respect the principles of impartiality, objectivity and neutrality and be exclusively guided by the interest of MONEYVAL. In doing so they shall be guided by the Principles of conduct for MONEYVAL Bureau members, working group co-chairs and scientific experts.

5. The Bureau may invite a representative of the FATF Steering Group, who is at the same time a member of a delegation to MONEYVAL, to be present at, and contribute to, Bureau meetings.

Rule 4 – Replacement of the Chair and the Vice-Chairs

1. If the Chair ceases to be a representative in MONEYVAL or resigns from the office, the Vice-Chair who has served the longest on the Bureau shall immediately and automatically become Chair for the period until elections can be held. If both Vice-Chairs have served on the Bureau for the same period, they should decide who replaces the Chair, in consultation with the Executive Secretary.

2. In cases set out under paragraph 1 or if a Vice-Chair becomes Chair pursuant to paragraph 1, or ceases to be a representative in MONEYVAL or resigns from his/her office, an election to fill the resulting vacancy shall take place as soon as possible.

3. If the offices of Chair and Vice-Chair are vacant at the same time, the duties of the Chair shall be carried out for the period until elections can be held by another representative sitting on the Bureau appointed after consultation with the remaining Bureau members and the Executive Secretary. Elections to fill the vacancies should take place as soon as possible[188].

4. If both the Chair and the Vice-Chairs are temporarily prevented from carrying out their duties, the duties of the Chair shall be carried out by another representative sitting on the Bureau according to the procedure outlined in paragraph 3 above.

Rule 5 – Limitation on the exercise of the functions of Chair

1. The Chair, a Vice Chair or any other representative carrying out the duty of the Chair, shall be replaced in the chair during the discussion and adoption of a report concerning their country/territory, or in any other situation where they are conflicted.

Rule 6 – Decision making procedures

Decision making on issues arising from Bureau discussions

1. The Bureau shall be entrusted with the tasks enumerated in Article 6 of the Statute of MONEYVAL, which shall be carried out through meetings of the Bureau or when appropriate, through teleconference or electronic exchanges.

2. Decisions by the Bureau shall be reached by consensus, which shall not be understood as requiring unanimity. When the Bureau has reached a decision in respect of a proposal to be made to the Plenary, the Chair shall present the collective decision of the Bureau members on behalf of all members.

Decision making on issues arising in reports elaborated under the evaluation procedures, including compliance reports and other assessments

3. Decisions on issues arising in mutual evaluation reports elaborated under the evaluation procedures, including compliance reports and other assessments shall be reached by a

[188] In accordance with Article 6 of CM/Res(2013)3 on the Statute of MONEYVAL the term of office of members of the Bureau is two years, renewable once. Any early election held for the office of Chair, Vice-Chair or Bureau member shall normally be held for a two-year term in accordance with the Statute. An election may be held for the remainder of the term of the resigning official (i.e. less than two years), however it shall not be counted into the total number of terms of the newly elected official, if the period of election (the new office term) is less than 1 year.

consensus of MONEYVAL countries and territories (which shall not be understood as requiring unanimity).

4. In order to assist the Chair in reaching a conclusion on the existence of consensus, discussions shall be based on substantiated opinions from the plenary, taking into account the views expressed by the evaluation team and the scientific experts.

5. If a consensus cannot be reached on the proposals to amend or otherwise change the draft report, including, where applicable, changes to proposed ratings, the report shall remain unchanged on the relevant issue. Where there are dissenting views, these can be reflected in the meeting report of the plenary upon the request of the dissenting country(ies) and/or territory(ies) concerned.

6. After consultation with the Bureau, the Chair may, when required, propose that the members take a decision when the Plenary is not in session through a "silent procedure" (i.e. the decision is adopted unless at least one delegation objects within a given timeframe[189]).This shall be limited to instances where the Chair considers that the adoption of that decision at the following Plenary would cause considerable inconveniences or practical difficulties. A suggestion to apply such a decision making progress shall be made in writing, with an indication of the exact time for the expiration. At the first meeting following the adoption of the decision, the Chair shall inform the Plenary on the procedure and the decision taken. The procedure shall not be applied for the adoption of a mutual evaluation report.

TITLE II. PROCEDURES CONCERNING MONEYVAL'S FIFTH ROUND OF EVALUATIONS

Chapter I – General principles and rules

Rule 7 – General provisions

1. The rules contained in the present title aim at further elaborating article 7 of the Statute of MONEYVAL. They should be periodically reviewed to identify on-going challenges and updated to address those challenges.

2. MONEYVAL shall conduct a fifth round of anti-money laundering and countering the financing of terrorism (AML/CFT) mutual evaluations for States and territories which are subject to its evaluation procedures, in order to assess their compliance with the relevant international AML/CFT standards, as set out in article 2 of the Statute of MONEYVAL.[190]

3. The evaluation procedure shall be based on the principle of mutual evaluation and peer pressure, and shall be instrumental in reaching the aims of MONEYVAL, as enshrined in Article 1 of the Statute. The evaluations shall be undertaken, taking into account the 2013 *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems*[191] (hereinafter "the Methodology"), as amended from time to time. The assessment of technical compliance shall address the extent to which the country or territory complies with the specific requirements of the standards in laws, regulations or other required measures, which are in force and in effect, including in respect

[189] When the "silent procedure" is applied for the adoption of follow-up reports, if two delegations (one of which might be the assessed country/territory) raises concerns, then that issue will be discussed at the Plenary.

[190] These are currently the 2012 Financial Action Task Force Recommendations (see http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf) and relevant international conventions referred therein.

[191] As set out in the Methodology, the scope of the evaluations involves 2 inter-related components for technical compliance and effectiveness. The technical compliance component assesses whether the necessary laws, regulations or other required measures are in force and effect, and whether the supporting AML/CFT institutional framework is in place. The effectiveness component assesses whether the AML/CFT systems are working, and the extent to which the country is achieving the defined set of outcomes.

of the institutional framework and the existence, powers and procedures of competent authorities. The assessment of effectiveness shall evaluate the adequacy of the implementation of the standards and identify the extent to which the country or territory achieves a defined set of outcomes that are central to a robust AML/CFT system.

4. A number of common general principles and objectives govern mutual evaluations and assessments conducted by the FATF, MONEYVAL, IMF, World Bank and other FATF-style regional bodies (FSRBs)[192]. In line with these principles and objectives, MONEYVAL's procedures should:

   a) produce objective and accurate reports of a high standard in a timely way;

   b) ensure that there is a level playing field, whereby mutual evaluation reports (MERs), including the executive summaries, are consistent, especially with respect to the findings, the recommendations and ratings;

   c) ensure that there is transparency and equality of treatment, in terms of the assessment process, for all countries and territories assessed;

   d) seek to ensure that MONEYVAL evaluations are equivalent with those conducted by all relevant organisations and bodies (FATF, IMF, World Bank, FSRBs), and of a high standard;

   e)

      (i) be clear and transparent,

      (ii) encourage the implementation of higher standards,

      (iii) identify and promote good and effective practices, and

      (iv) alert governments and the private sector to areas that need strengthening;

   f) be sufficiently streamlined and efficient to ensure that there are no unnecessary delays or duplication in the process and that resources are used effectively.

5. Mutual evaluation reports shall reflect the situation in the country or territory at the time of the on-site visit. The assessment process will take into account relevant laws, regulations or other AML/CFT measures that are in force and effect at that time, or will be in force and effect by the end of the on-site visit.

Rule 8 – Changes and interpretation of the AML/CFT standards

1. As a dynamic process, on-going work within the FATF and the European Union could lead to further changes to the relevant standards and/or the methodology. All countries and territories should be evaluated on the basis of the Standards and Methodology as they exist at the date of the country/territory's on-site visit. The report shall state clearly if an assessment has been made against recently amended standards. To ensure equality of treatment, and to protect the international financial system, compliance with the relevant elements of the changes could be assessed as part of the follow-up process, if they have not been assessed or as part of the mutual evaluation.

2. As necessary, MONEYVAL may take up issues pertinent to the interpretation and implementation of the standards by means of the mechanism established by the FATF for this purpose. Where the horizontal issue cannot be resolved at the FSRB level they it shall be initially raised by the MONEYVAL Secretariat with the FATF Secretariat. The MONEYVAL Plenary shall be kept informed of such exchanges. The Plenary may then decide to raise an issue more formally with the FATF. In this case the issue should present important and relevant procedural or substantive matters stemming from one or multiple MERs or FURs, and on which there has been no clear interpretation by the FATF. The MONEYVAL Chair shall

[192] See FATF and FSRB's agreed universal procedures for assessments conducted by assessment bodies (February 2016).

write to the FATF at the appropriate level outlining the issue and requesting a formal interpretation from the FATF. Based on Plenary considerations, the MONEYVAL Secretariat shall prepare a background analysis to accompany the request, outlining the impact that the issue, if left unaddressed, could have an impact on the mutual evaluation process of MONEYVAL.

Rule 9 – Schedule for the fifth round

1. The schedule of mutual evaluations for the fifth round, and the number of evaluations to be prepared each year is primarily governed by the resources available to undertake these evaluations, the number of MERs that can be discussed at each Plenary meeting, and by the need to complete the entire round in a reasonable timeframe. The number of MERs to be discussed at each Plenary should not exceed 3.
2. A schedule of mutual evaluations showing the fixed or proposed date of the on-site visit, of relevant Financial Sector Assessment Programme (FSAP) missions and the date for the Plenary discussion of the MER will be maintained. The considerations underlying the sequence of evaluations were:
   a) the sequence of evaluations following the previous round of evaluations (or International Financial Institution (IFI) assessment) and date of the last assessment;
   b) countries' and territories' views on the proposed date (delegations are consulted on the possible dates for on-site visits and Plenary discussion of their MER);
   c) results of the previous mutual evaluation or progress or lack thereof as a result of follow-up processes;
   d) the scheduled date of any possible FSAP mission by the IFIs;
   e) issues arising from the last round which may indicate that a further evaluation should be a priority; and
   f) that fact that a country or territory has not participated in MONEYVAL's 4th round.
3. The sequence of evaluations shall retain flexibility in order to ensure that the evaluation process can respond appropriately and in timely fashion to the needs of the membership and to concerns in the global network of AML/CFT assessment bodies. The Chair and the Executive Secretary should be informed in due course by the respective delegation where any such concerns arise.
4. When it is known sufficiently in advance (i.e. for at least 6 months) that a MONEYVAL country/territory is to undergo a Financial Sector Assessment (FSAP),[193] the order of

[193] The FATF Standards are recognised by the IFIs as one of twelve (12) key standards and codes, for which Reports on Observance of Standards and Codes (ROSCs) are prepared, often in the context of a Financial Sector Assessment Programme (FSAP). It is mandatory for jurisdictions with systemically important financial sectors to undergo financial stability assessments under the FSAP every five (5) years. Under current FSAP policy, every FSAP and FSAP update should incorporate timely and accurate input on AML/CFT. Where possible, this input should be based on a comprehensive quality AML/CFT assessment and, in due course, in the case of MONEYVAL, on a follow-up assessment, conducted against the prevailing standard. MONEYVAL and the IFIs should therefore co-ordinate with a view to ensuring a reasonable proximity between the date of the FSAP mission and that of a mutual evaluation or a follow-up assessment conducted under the prevailing methodology, to allow for the key findings of that evaluation or follow-up assessment to be reflected in the FSAP; and members are encouraged to co-ordinate the timing for both processes internally, and with the MONEYVAL Secretariat and IFI staff. If necessary, the staff of the IFIs may supplement the information derived from the ROSC to ensure the accuracy of the AML/CFT input. In instances where a comprehensive assessment or follow-up assessment against the prevailing standard is not available at the time of the FSAP, the staff of the IFIs may need to derive key findings on the basis of other sources of information, such as the most recent assessment report, and follow-up and/or other reports. As necessary, the staff of the IFIs may also seek updates from the authorities or join the FSAP mission for a review of the most significant AML/CFT issues for the country in the context of the prevailing standard and methodology. In such cases, staff would present the key findings in the FSAP documents; however, staff would not prepare a ROSC or ratings.

evaluations can be departed from so that a MONEYVAL evaluation can be completed with a view to it being used as the AML/CFT component in the FSAP, thus avoiding duplication.

Rule 10 – Respecting Timelines

1. The assessed countries and assessment teams have the flexibility to extend the overall timeline by up to one or 2 months in order to take into consideration the scheduled dates of MONEYVAL Plenary meetings, events or holidays, or to adjust the date of the on-site visit to the most appropriate time. When translation is needed, assessment bodies should ensure that 4 extra weeks are scheduled for translation purposes. In practice, this may require an earlier start to the evaluation process as there is no scope for reducing the time allocated to the post-onsite stages of the process, and the assessed country and assessment team should therefore agree on the broad timeline of the evaluation at least 14 months before the scheduled MONEYVAL Plenary discussion of the evaluation report.
2. The timelines are intended to provide guidance on what is required if the reports are to be prepared within a reasonable timeframe, and in sufficient time for discussion in Plenary. It is therefore important that the assessors, the secretariat, the reviewers and the country/territory respect the timelines. Delays may significantly impact the ability of the Plenary to discuss the report in a meaningful way. The draft schedule of evaluations has been prepared so as to allow enough time between the on-site visit and the Plenary discussion.
3. The country/territory, the secretariat, the assessors and the reviewers undertake to meet the necessary deadlines and to provide full, accurate and timely responses, reports or other material as required under the agreed procedure.
4. Where there is a failure to comply with the agreed timelines, then the following actions could be taken (depending on the nature of the default):

    a) **Failure by the country/territory** - Failure to comply with the time deadline or to provide full and accurate responses may result in the visit being deferred and the evaluators being informed of this, and the consequent need for materials to be updated at a later stage. A decision to defer the evaluation in either of these circumstances shall be taken by the Chairman, after discussions with the Head of the relevant Delegation, and in consultation with the Executive Secretary. The country/territory shall be advised in writing of this decision, and the letter will be copied to other Heads of delegation and observers. The Director General of Human Rights and Rule of Law of the Council of Europe may also be invited to write to the responsible Minister or draw the matter to the attention of the Permanent Representative to the Council of Europe of the assessed country/territory. In addition, the assessment team may have to finalise and conclude the report based on the information available to them at that time.

    b) **Failure by the assessors, the reviewers or the secretariat** - the Chairman may write a letter to or liaise with the head of delegation of the reviewer or the Executive Secretary (for the secretariat). If the written contribution(s) from assessors are not received within the agreed timescales, or if they do not meet the minimum quality requirements, the secretariat shall notify the Bureau and the head of delegation of the evaluating State or territory. The Head of Delegation will use his//her best endeavours to ensure that the required assessor's contribution, or in appropriate cases a substantially revised contribution is sent to the secretariat within 2 weeks from the notification.[194] In the event that a substantial contribution has still not been received

[194] When an assessor must leave the assessment due to *force majeure,* or her/his submission is delayed or not submitted, the responsibilities for the respective parts of the assessment shall be reallocated to other members of the assessment team with the support of the Secretariat. If an assessor departs the team prior to the on-site visit the Secretariat shall endeavour to find a replacement assessor as soon as possible.

from the relevant assessor, the Chairman shall formally draw this issue to the attention of the Permanent Representative to the Council of Europe of the assessor's State or territory, with copies of the letter being sent to the assessor concerned and his/her Head of Delegation.

5. The secretariat shall keep the Chairman informed of any failures so that the Chairman can respond in an effective and timely way. The Plenary is also to be informed if the failures result in a request to delay the discussion of the MER, including as to reasons for deferral, and publicity could be given to the deferment (as appropriate) or other additional action considered. In addition, the assessment team may have to finalise and conclude the report based on the information available to them at that time.

Rule 11 – Joint mutual evaluations with the FATF and related follow-up

1. Mutual evaluations of MONEYVAL countries/territories which are also members of the FATF shall be undertaken pursuant to the procedures agreed by the FATF (Procedures for the FATF 4th round of AML/CFT evaluations).[195] These procedures shall also be applied in the context of the follow-up processes.

2. MONEYVAL countries/territories shall be given the opportunity to participate in the evaluation process directly through being part of the assessment team (which shall include MONEYVAL assessors and the secretariat) and also by being able to provide comments and input as is possible for FATF delegations. The secretariat shall ensure that the relevant evaluation documents are circulated for comments and input to all MONEYVAL countries/territories and that the comments received shall be communicated to the FATF as appropriate. Based on reciprocity, FATF members shall also be able to participate in mutual evaluation discussions of joint FATF/MONEYVAL members' reports within MONEYVAL.

3. The first discussion of the MER shall take place in the FATF, unless otherwise jointly agreed. The presumption is that the FATF's view on the draft MER shall be conclusive. However, in exceptional cases, where a report was agreed within the FATF but subsequently MONEYVAL identifies major difficulties with the text of the report, the Plenary shall request the Executive Secretary to communicate to the FATF the issues identified less than four to six weeks before the FATF Plenary so that these can be discussed at the following FATF Plenary.

Rule 12 – IMF or World Bank led assessments and other coordination aspects

1. MONEYVAL is responsible for the mutual evaluation process for all of its countries/territories and shares this responsibility with the FATF as far as joint members are concerned. Subject to the provisions of Rule 11, there is thus a presumption that MONEYVAL will conduct the respective mutual evaluations, including any follow-up that may be required, as part of this process. The presumption can be overridden at the discretion of the MONEYVAL Plenary on a case by case basis, with the country/territory's agreement.

2. For the purposes of the 5th round of mutual evaluations, the MONEYVAL Plenary has discretion as to the number of MONEYVAL assessments that could be conducted by the IFIs (i.e. IMF or World Bank). Such IFI-led assessments should be agreed and fixed on the same basis as other evaluations in the schedule.

3. For the MONEYVAL assessment schedule to be fixed with appropriate certainty and in a coordinated manner, the process leading to the Plenary decision as to which MONEYVAL countries/ territories will have an assessment led by an IFI team should be clear and transparent. In order for the evaluation schedule to be appropriately planned and assessment teams to be formed in sufficient time, it will be necessary for MONEYVAL to be involved at an early stage in the process of determining which countries and territories will be assessed by

[195] See http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF-4th-Round-Procedures.pdf

an IFI. The Plenary will be informed on a regular basis as to the current status of the assessment schedule, including proposals as to whether assessments will be IFI-led, and the Plenary will decide on any such requests. Where the IMF or WB conduct an AML/CFT assessment as part of the MONEYVAL 5th round, they should use procedures and a timetable similar to those of MONEYVAL.

4. The MONEYVAL Plenary will in all cases have to approve an IFI assessment that is conducted under the MONEYVAL 5th round for it to be accepted as a mutual evaluation.

5. MONEYVAL should be given the opportunity to participate in the evaluation process directly through being part of the assessment team (which shall include at least one MONEYVAL assessor) and, subject to available resources, a MONEYVAL secretariat member.

6. Furthermore, a country or territory agreeing to an IFI-led evaluation shall consent to provide to the MONEYVAL secretariat a copy of all evaluation documentation communicated to the IFI, as well as a copy of the draft reports and comments made by the delegation on the draft text, at the key stages of the evaluation process.

7. The basic products of the evaluation process are the MER and the Executive Summary (for MONEYVAL) and the Detailed Assessment Report (DAR) and the ROSC (for the IFIs).[196] The Executive Summary, whether derived from a MER or a follow-up assessment report (see Rules 21 and 24 below), will form the basis of the ROSC. Following the Plenary, and after the finalisation of the Executive Summary, the summary is provided by the secretariat to the IMF or World Bank so that a ROSC can be prepared following a pro forma review.

8. The substantive text of the draft ROSC will be the same as that of the Executive Summary, though a formal paragraph will be added at the beginning:

   "This Report on the Observance of Standards and Codes for the *FATF Recommendations and Effectiveness of AML/CFT Systems* was prepared by MONEYVAL. The report provides a summary of AML/CFT measures in place in [*Country/territory*] as at [*date*], the level of compliance with the FATF Recommendations, the level of effectiveness of the AML/CFT system, and contains recommendations on how the latter could be strengthened. The views expressed in this document have been agreed by MONEYVAL and [*Country/territory*], but do not necessarily reflect the views of the Boards or staff of the IMF or World Bank."

9. MONEYVAL's confidentiality and publication rules apply equally for such assessments. Consideration shall be given to the timing of publication of MERs, with a view to finding a mutually agreed publication date with the IFI having conducted the assessment.

Rule 13 – Identification of any quality or consistency issues in respect of mutual evaluations

Quality & consistency review of MONEYVAL reports

1. A quality and consistency review shall be carried out through a mechanism involving MONEYVAL scientific experts, experts serving on the Ad Hoc Group of experts (appendix 2). The main functions of the reviewers are further detailed in Appendix 2.

2. The review will involve drawing on expertise from several qualified volunteer experts, based on their professional experience, expertise as assessors and their knowledge of the AML/CFT specificities. This pool may contain experts from MONEYVAL, FATF and FSRB members, including their secretariat members, and observers. Each review shall involve at least one external reviewer. To avoid potential conflicts, the reviewers selected for any given quality and consistency review will be from countries other than those of the assessors and will be made known to the country and assessors in advance. Due to the nature of the peer review

[196] The DAR uses a similar template to that of the common agreed template that is annexed to the Methodology and has the same format.

process, the secretariat will work to ensure that the mutuality of the process is maintained, and all delegations should propose qualified experts as reviewers. A list of past and potential reviewers will be maintained by the secretariat.

3. The reviewers will need to be able to commit time and resources to review the scoping note and the quality, coherence and internal consistency of the draft MER, as well as consistency with the standards and precedents. The reviewers for the quality and consistency review do not have any decision-making powers or powers to change a report.

Quality and consistency review of mutual evaluation reports of another assessment body

4. Where a MONEYVAL country/territory or the MONEYVAL Secretariat, considers that a draft MER[197] of another assessment body of the global AML/CFT network has serious or major issues of quality or consistency (e.g. where ratings are clearly inappropriate, are not consistent with the analysis, where there has been a serious misinterpretation of the Standards or the Methodology, or where an important part of the Methodology has been systematically misapplied), it should, wherever possible, raise such concerns~~,~~ through its Chairman or Executive Secretary, with the assessment body conducting the assessment prior to the MER's adoption by that body.

5. In such cases, the Executive Secretary of MONEYVAL should be notified without delay by the respective MONEYVAL country/territory, indicating in writing the issues of specific concern. The Executive Secretary shall immediately notify the Chairman and Heads of delegations, with a view to reaching a decision as soon as possible as to whether the concerns expressed qualify under this procedure. This consultation shall take place when necessary, through an electronic procedure, if there is no Plenary meeting within a reasonable timeframe. The scientific experts may also be consulted in this process when necessary. If MONEYVAL decides that there are significant concerns, it shall notify the FATF secretariat and the secretariat of the relevant assessment body, so that the assessment team and assessed country can consider and work to appropriately address the concerns.

6. The MONEYVAL secretariat shall ensure that the adopted MER will be circulated to all MONEYVAL heads of delegations. Where there remain significant concerns about the quality and consistency of a MER of another assessment body after its adoption, MONEYVAL should inform the assessment body and the FATF secretariat in writing about those concerns **within 2 weeks** of the distribution of the MER following adoption. If a delegation has serious concerns about the quality and consistency of the MER, the Head of delegation should advise **within 10 days** the MONEYVAL Executive Secretary, in writing, indicating their specific concerns. The Executive Secretary shall refer those concerns to the FATF secretariat. Such cases shall be considered following the FATF's rules for ex-post review of major quality and consistency problems.[198]

Chapter II – Preparatory measures and on-site evaluation

Rule 14 – Preparation for the on-site visit

1. A country or territory should normally be made aware of the dates of their evaluation, as scheduled in the evaluations calendar, **at least 1 year** in advance. At that time, the country/territory should indicate an identified contact person or point for the assessment with whom the secretariat shall liaise for the preparation for the on-site evaluation visit. The Secretariat will fix the precise dates for the evaluation on-site visit **at least 6 months** or as early as possible, before the on-site visit, together with the timelines for the whole process,

[197] References to MER include also detailed assessment reports prepared by IFIs.

[198] For such concerns to be considered further in the process, any specific concern should be raised by at least 2 of any of the following: FATF or FSRB members or secretariats, or IFIs; at least one of which should have taken part in the adoption of the MER.

in consultation with the country/territory (some flexibility is permissible). The country or territory will advise whether they wish to conduct the evaluation in English or French.

2. **At least 9 months** in advance, the secretariat will communicate to the country/territory's designated contact person the relevant template questionnaires as revised from time to time. The onus is on the country/territory to demonstrate that it has complied with the Standards and that its AML/CFT regime is effective. Thus, the country/territory should provide all relevant information to the assessment team during the course of the assessment. As appropriate, assessors shall be able to request, through the secretariat, or access documents (redacted if necessary), data, or other relevant information.

3. All information should be provided in an electronic format, including a full response to the template questionnaires. Countries/territories should ensure that laws, regulations, guidelines and other relevant documents that are referenced in the completed questionnaires are adequately translated in the language of the evaluation[199] and are made available in advance of the on-site visit. When additional information is provided at a later stage, this information should be supported by relevant documents and the country/territory must ensure prompt translation into the language of the evaluation.

(a) Information Updates on Technical Compliance

4. The information provided by the assessed country/territory is intended to provide key information for the preparatory work before the on-site visit, including understanding the country/ territory's ML/TF risks, identifying potential areas of increased focus for the on-site, and preparing the draft MER. Countries and territories should provide the necessary information to the secretariat **no less than 6 months before the on-site**.

5. In some countries and territories, AML/CFT issues are matters that are addressed not just at the level of the national government, but also at state/province or local levels. Countries/ territories are requested to note where the AML/CFT measures are the responsibility of state/provincial/local level authorities, and to provide an appropriate description of these measures. Assessors should also be aware that AML/CFT measures may be taken at one or more levels of government, and should examine and take into account all the relevant measures, including those taken at a state/provincial/local level. Equally, assessors should take into account and refer to supra-national laws or regulations that apply to a country/territory.

6. Countries/territories should rely on the template questionnaire for the technical compliance to provide relevant information to the assessment team. Along with previous reports, this will be used as a starting point for the assessment team to conduct the desk-based review of technical compliance supported by the secretariat. The questionnaire is a guide to assist countries/territories to provide relevant information in relation to: (i) background information on the institutional framework; (ii) information on risks and context; (iii) information on the measures that the country/territory has taken to meet the criteria for each Recommendation. Countries/territories should complete the questionnaire and may choose to present additional information in whatever manner they deem to be most expedient or effective.

(b) Information on Effectiveness

7. Countries/territories should rely on the template questionnaire to provide relevant information to the assessment team on effectiveness, based on the 11 Immediate Outcomes identified in the effectiveness assessment **no less than 5 months before the on-site**. They should set out fully how each of the core issues is being addressed as set out in each

[199] The authorities should ensure that translations provided to the evaluation team are official translations or otherwise that the adequacy of the translation and use of specialised terminology has been checked by the relevant institutions prior to its submission to the evaluation team for assessment.

Immediate Outcome. It is important for countries/territories to provide a full and accurate description (including examples of information, data and other factors) that would help to demonstrate the effectiveness of the AML/CFT regime. Countries/territories should complete the questionnaire and may choose to present additional information in whatever manner it deems to be most expedient or effective.

(c) Composition and Formation of Assessment Team

8. The assessors will be selected by the secretariat, consulting as necessary with the Chairman and other Bureau members. This will normally take place **at least 6 months before the onsite**. The Executive Secretary will formally advise the country/territory of the composition of the assessment team at the time the team is confirmed. In case of a principled and reasoned objection by the country or territory, the secretariat, in consultation with the Chairman, may submit an alternative proposal.

9. An assessment team will usually consist of at least 4 expert assessors (comprising at a minimum one legal, financial[200] and law enforcement expert), principally drawn from MONEYVAL countries and territories and will be supported by members of the MONEYVAL Secretariat. Depending on the country/territory assessed and the money laundering and terrorist financing risks, additional assessors or assessors with specific expertise may also be required, including where possible evaluators from an FATF country. In selecting the assessors, a number of factors will be considered: (i) their relevant operational and assessment experience; (ii) language of the evaluation; (iii) nature of the legal system (civil law or common law) and institutional framework; and (iv) specific characteristics of the jurisdiction (e.g. size and composition of the economy and financial sector, geographical factors, and trading or cultural links), to ensure that the assessment team has the correct balance of knowledge and skills. Assessors should be very knowledgeable about the FATF Standards and Methodology, and are required to successfully complete an assessor training seminar before they conduct a mutual evaluation. Usually, at least one of the assessors should have had previous experience conducting an assessment.

10. For some evaluations, the secretariat could invite an expert from observer organisations or bodies[201] to participate on the assessment team, on the basis of reciprocity. Participation of an observer in the assessment process shall be subject to prior agreement by the country or territory assessed.

11. Due to the nature of the peer review process, the secretariat will work to ensure so far as it is possible that the mutuality of the process is maintained, and MONEYVAL countries and territories should provide qualified experts over the course of the fifth round. A list of assessors shall be maintained by the secretariat, and updated on a regular basis, based on information on modifications notified by the Head of Delegation. Heads of delegations shall use their best endeavours to ensure that experts within their jurisdiction are available for assessor training and to participate in MONEYVAL evaluations and provide their written reports.

(d) Responsibilities of the Secretariat

12. The Secretariat

- Supports the assessment team and the assessed country;

[200] The assessment team should have assessors with expertise relating to the preventive measures necessary for the financial sector and designated non-financial businesses and professions.

[201] Participation (on a reciprocal basis) of experts from other observers that are conducting assessments, such as the FATF (member or Secretariat), the IMF/World Bank, UNCTED, other FSRBs (Secretariat) could be considered on a case by case basis.

- Focuses on quality and consistency, including taking steps necessary to ensure that the assessors' analysis is clearly and concisely written, comprehensive, objective and supported by evidence;
- Ensures compliance with process and procedures;
- Assists assessors and assessed country in the application of the standards, methodology and process in line with written interpretation provided by the FATF and, where relevant, taking into account past MONEYVAL Plenary decisions and horizontal analysis;. Where a particular horizontal issue has been identified as requiring interpretation, the Secretariat shall request the FATF for an interpretation in accordance with paragraph 2, Rule 8 of these Procedures;
- Ensures that assessors and assessed countries have access to relevant and accurate documentation, and checks that statistics and legislative references are cited correctly;
- Project-leads the process and other tasks as indicated in these procedures.

(e) Responsibilities of the Assessment Team (assessors)

13. The assessment team is coordinated by a member of the secretariat, who shall ensure that the assessment team collectively produces an independent report (containing analysis, findings and recommendations) concerning the country/territory's compliance with the relevant international standards, in terms of both technical compliance and effectiveness. If possible, a preparatory meeting between the secretariat and assessors shall be organised in advance of the on-site visit.

14. A successful assessment of an AML/CFT regime requires, at a minimum, a combination of financial, legal and law enforcement expertise, particularly in relation to the assessment of effectiveness. Experts therefore have to conduct an evaluation in a fully collaborative process, whereby all aspects of the review are conducted holistically. Each expert is expected to contribute to all parts of the review, but should take the lead on, or take primary responsibility for topics related to his or her own area of expertise. An overview of assessors' respective primary responsibilities should be shared with the assessed country, even if the assessment remains an all-team responsibility. As a result, assessors will be actively involved in all areas of the report and beyond their primary assigned areas of responsibilities. It is also important that assessors are able to devote their time and resources to reviewing all the documents (including the information updates on technical compliance, and information on effectiveness), raising queries prior to the on-site, preparing and conducting the assessment, drafting the MER, attending the meetings (e.g. on-site, face-to-face meeting, and Plenary discussion), and adhere to the deadlines indicated.

15. The mutual evaluation is a dynamic and continuous process. The secretariat shall engage and consult the assessed country/territory on an on-going basis, commencing **at least 9 months** before the on-site. Throughout the process, the secretariat will ensure that the assessors can access all relevant material and that regular conference calls take place between assessors and the assessed country so as to ensure a smooth exchange of information and open lines of communication. This may include early engagement with higher level authorities to obtain support for and co-ordination of the evaluation for the entirety of the process and training for the assessed country to familiarise stakeholders with the mutual evaluation process. The Plenary should review from time to time, whether there is satisfactory engagements with assessed jurisdictions. Assessed jurisdictions should consider appointing, at an early stage in the evaluation process, a co-ordinator responsible for the mutual evaluation process to ensure adequate co-ordination and clear channels of communication between the secretariat and the assessed jurisdiction. The co-ordinator should have the appropriate seniority to be able to co-ordinate with other authorities effectively and make certain decisions when required to do so. The co-ordinator should also have an understanding of the mutual evaluation process and be able to perform quality control of responses provided by other national authorities.

(f) Desk-Based Review for Technical Compliance

16. Prior to the on-site visit, the assessment team will conduct a desk-based review of the country/territory's level of technical compliance, and the contextual factors and ML/TF risks, supported by the secretariat.The review will be based on information provided by the country/territory in the information updates on technical compliance, pre-existing information drawn from the country's evaluation reports, follow-up reports and other credible or reliable sources of information (e.g. reports from other international organisations). This information will be carefully taken into account, though the assessment team can review the findings from the previous MER and follow-up reports, and may highlight relevant strengths or weaknesses not previously noted. If the assessment team reach a different conclusion to previous MERs and follow-up reports (in cases where the Standards and the legislation have not changed) then they should explain the reasons for their conclusion.

17. The technical compliance annex is drafted by the assessment team, supported by the Secretariat. This requires assessors to indicate if each criterion and sub-criterion is met, mostly met, partly met or not met and why. Subsequent to the review, the assessment team will provide the country or the territory with a 1st draft of the technical compliance annex (which need not contain ratings or recommendations) about 3 months before the on-site. This will include a description, analysis, and list of potential technical deficiencies noted. The country/territory will have one month to clarify and comment on this 1st draft on technical compliance annex.

18. In conducting the assessment, assessors should only take into account relevant laws, regulations or other AML/CFT measures that are in force and effect at that time, or will be in force and effect by the end of the on-site visit. Where relevant bills or other specific proposals to amend the system are made available these will be referred to in the MER (including for the purpose of the recommendations to be made to the country) but should not be taken into account in the conclusions of the assessment or for ratings purposes.

(g) Ensuring Adequate Basis to Assess International Co-operation and Areas of Higher Risks

19. **6 months before the on-site visit**, the secretariat will invite MONEYVAL countries/territories, FATF members and FSRBs to provide information on their experience of international co-operation with the country/territory being evaluated, or any other AML/CFT issues that they would like to see raised and discussed during the on-site visit. They will also be invited to provide information that would assist the team to identify and focus on areas of higher or lower risks that need increased focus.

20. In addition, the assessment team and the country/territory may also identify key countries and territories which the assessed country/territory has provided international cooperation to or requested it from and seek specific feedback. The feedback could relate to: (i) general experience, (ii) positive examples, and (iii) negative examples, on the assessed country's level of international cooperation. The responses received will be made available to the assessment team and the assessed country/territory.

(h) Identifying Potential Areas of Increased Focus for On-Site Visit

21. The assessment team will have to examine the country/territory's level of effectiveness in relation to all the 11 Immediate Outcomes during the on-site. Prior to the on-site visit, the assessment team will, based on its preliminary analysis (of both technical compliance and effectiveness issues), identify specific areas which it would pay more attention to during the on-site visit and in the MER. This will usually relate to effectiveness issues but could also include technical compliance issues. In doing so, the team will consult the country/territory and take into consideration the information provided in this respect by other delegations.

22. Where there are potential areas of increased or reduced focus for the on-site, the assessment team should obtain and consider all relevant information and commence discussion of these areas **approximately 4 months before the on-site**, and the secretariat should consult the country/territory **at least 2 months** before the on-site. The country/territory should normally provide additional information regarding the areas which the assessment team would like to pay more or less attention to. While the prerogative lies with the assessment team, the areas for increased or reduced focus should, to the extent possible, be mutually agreed with the country/territory. The scoping note should set out briefly (in no more than 2 pages) the areas for increased and reduced focus, and the rationale. The draft scoping note, along with relevant background information (e.g. the country/territory's risk assessment(s)), should be sent to the reviewers (described in the section on quality and consistency, below) and to the country/territory. Reviewers should, **within one week** of receiving the scoping note, provide their feedback to the assessment team regarding whether the scoping note reflects a reasonable view on the focus of the assessment, having regard to the material made available to them as well as their general knowledge of the jurisdiction. The assessment team should consider the merit of the reviewers' comments, and amend the scoping note as needed. The secretariat should send the final version to the country/territory, **at least 4 weeks prior to the on-site**, along with any requests for additional information on the areas of increased or reduced focus. To expedite the mutual evaluation process, and to facilitate the on-site visit, the assessment team will, one week before the on-site visit, prepare a revised draft TC annex, and an outline of initial findings/key issues to discuss on effectiveness. In order to facilitate the discussions on-site, the secretariat will send the revised TC annex to the country/territory at that time.

(i) Programme for On-Site Visit (Pre-Plenary)

23. The country/territory (designated contact) should work with the secretariat and prepare a draft programme and coordinate the logistics for the on-site. The draft programme, together with any specific logistical arrangements, should be sent to the secretariat no later than 8 weeks before the visit. Please see Appendix 1 for the list of authorities and businesses that would usually be involved in the on-site.

24. To assist in preparation, the assessment team should prepare itself for the on-site by developinga preliminary analysis identifying key issues on effectiveness[202], 4 weeks before the onsite.

25. The draft programme should take into account the areas where the assessment team may want to apply increased or reduced focus. Where practical, meetings could be held in the premises of the agency/organisation being met, since this allows the assessors to meet the widest possible range of staff and to obtain information more easily. However, for some evaluations travelling between venues can be time consuming and wasteful, and generally, unless venues are in close proximity, there should be no more than 2 to 3 venues per day. The programme should be finalised at least 3 weeks prior to the on-site visit. The assessment team may also request additional meetings during the on-site.

26. Both in terms of the programme and more generally, the time required for interpretation, and for translation of documents, must be taken into account. During the on-site visit there also needs to be independent, professional and well-prepared interpreters if interpretation into English or French is required. However, for the efficient use of time, meetings should generally be conducted in the language of the assessment. The cost of interpretation and other necessary equipments hall be borne by the assessed country/territory, which is responsible for testing that systems work in advance. If there is a problem with organising interpretation, the assessed country/territory should inform the secretariat at least one month in advance of the on-site visit.

[202] This should normally include a list of preliminary findings and questions per each Core Issue.

Rule 15 – On-site visit

1. The on-site visit provides the best opportunity to clarify issues relating to the country/territory's AML/CFT system, and assessors need to be fully prepared to review the 11 Immediate Outcomes relating to the effectiveness of the system and clarify any outstanding technical compliance issues. Assessors should also pay more attention to areas where higher money laundering and terrorist financing risks are identified. Assessors must be cognisant of the different country/territory circumstances and risks, and that countries and territories may adopt different approaches to meet the relevant international standards and to create an effective system. Assessors thus need to be open and flexible and seek to avoid narrow comparisons with their own national requirements.

2. Each on-site visit will normally be conducted over a period which is likely to be **between 10 and 14 days**, or longer as appropriate. A typical on-site visit would allow for the following:

   - An initial half day preparatory meeting between the secretariat and assessors;
   - Meetings[203] with relevant officials and representatives of the assessed country, including an opening and closing meeting. The opening meeting should include an overview of the country's understanding of risk, to complement the write-ups of the country's national risk assessment(s). Time may have to be set aside for additional or follow-up meetings, if, in the course of the set schedule, the assessors identify new issues that need to be explored, or if they need further information on an issue already discussed.
   - One to 2 days where assessors work on the draft MER (supported by the Secretariat), to ensure that all the major issues that arose during the evaluation are noted in the MER, and discuss preliminary ratings, and key recommendations.

3. It is important that the assessment team be able to request and meet with all relevant agencies during the on-site. The country/territory being evaluated, and the specific agencies met should ensure that appropriate staff[204] are available for each meeting. The assessment team should be provided with a specific office for the duration of the on-site mission, and the room should have photocopying, printing and other basic facilities, as well as internet access.

4. Meetings with the private sector or other non-government representatives[205] are an important part of the visit. The assessors shall be given the opportunity to meet with such bodies or persons in private, and without an official present. When the coordinating institution wishes to have an official attend other meeting than those of its own institution, the official shall be able to take part in those meetings, only at the discretion of the assessment team and in an observer capacity.

5. The assessment team shall provide a written summary of its key findings to the assessed country/territory officials at the closing meeting. With the permission of the country/territory undergoing evaluation, the key findings may be passed by the secretariat to the IMF or World Bank, if it is required to assist with an FSAP mission planned or in progress.

Chapter III – Post-visit procedure

Rule 16 – Post on-site - preparation of draft Executive Summary and MER

[203] The assessment team should also set aside time midway through the on-site to review the progress of the mutual evaluation and where relevant, the identified areas of increased focus for the on-site initially.

[204] While the level and seniority of officials may vary from agency to agency, generally speaking, countries and territories shall ensure that both senior managers who are engaged with the institution that they are representing at a policy level, as well as operational staff who can respond to detailed questions on AML/CFT implementation are present at each meeting.

[205] E.g. those listed in Appendix 1.

1. There should be a minimum of 27 weeks between the end of the on-site visit and the discussion of the MER in Plenary. The timely preparation of the MER and Executive Summary[206] will require the assessors to work closely with the secretariat and the country/territory. Depending on when the Plenary discussion is scheduled, the time period may also be extended or adjusted. In exceptional cases and based on justified circumstances (and with the consent of the assessed country), a shorter period of time may be allowed for.

2. The steps in finalising a draft report for discussion at Plenary, and the approximate time that is required for each part, are set out in greater detail below.

3. With the aim to facilitate communication between the assessment team and the assessed country, the Secretariat should facilitate regular conference calls between all relevant parties, in particular after the circulation of an updated draft MER. In the course of drafting the first and second draft MER, assessors should aim to clarify as much as possible, in written or orally, if and how information submitted by the assessed country was taken into account and if/where additional information is still needed.[207]

1st Draft MER

4. The secretariat and assessment team will have **6 weeks** to coordinate and refine the 1st draft MER (including the key findings, and recommended actions to the country).

5. The secretariat will send the 1st draft MER to the country/territory for comments. The country/territory will have **4 weeks** to review and provide its comments on the 1st draft MER to the secretariat. During this time, the assessment team would have to be prepared to respond to queries and clarifications that may be raised by the country/territory.

2nd Draft MER and Executive Summary

6. On receipt of the country's comments on the 1st draft MER, the assessment team will have 4 weeks to review the various comments and make further amendments, and begin drafting the Executive Summary. Every effort should be made to ensure that the revised draft is as close to a draft MER as possible, acknowledging that there are still further opportunities for amendment. The 2nd draft MER and draft Executive Summary will then be sent to the country and to the reviewers (approximately 14 weeks after the on-site).

Meeting with the evaluation team

7. When possible, either before or after the finalisation of the 2nd Draft MER the secretariat may organise a 1-2 days meeting for the evaluation team to work on the draft MER, to ensure that all the major issues that arose during the evaluation are noted in the report, and discuss and agree the preliminary recommendations and ratings.

Internal quality and consistency review

8. The reviewers shall provide their comments on the 2nd draft MER **within 2 weeks (or 3 weeks where possible)** to the secretariat for communication to the assessment team. To assist their task, they will receive a copy of the comments provided by the country/territory on the 1st draft MER. The reviewers' comments will be disclosed to the assessors and assessed country/territory. It is the responsibility of the assessment team to consider the reviewers' comments and then decide whether any changes should be made to the report. The assessment team should provide to the Plenary a document containing short responses on the decisions and changes it has made to the report based on the reviewers' comments, and the Secretariat should liaise with external reviewers as needed to facilitate this process. The

[206] The format for the Executive Summary and MER is contained in Annex II of the Methodology. Assessors should also pay attention to the guidance on how to complete the Executive Summary and MER, including with respect to the expected length of the MER (100 pages or less, together with a technical annex of up to 60 pages).

[207] Assessors need not include all the information submitted by the assessed country, and should exercise discretion in determining which information are the most relevant to be included.

Secretariat will engage the assessed country to discuss further changes to the draft MER, and identify issues for discussion at the face-to-face meeting or video/teleconference.

Rule 17 – Face-to-Face Meeting

1. A face-to-face meeting is an important way to assist the country/territory and assessment team to resolve outstanding issues. Hence, the secretariat will arrange a face-to-face meeting between the assessment team and the country/territory to further discuss the draft MER and Executive Summary before it is circulated to the Plenary. During this session, the assessment team and country/territory shall work to resolve any major issues raised by reviewers as well as any major disagreements over technical compliance or effectiveness issues and identify potential priority issues for Plenary discussion. The face-to-face meeting should occur at least 8 weeks before the Plenary (i.e. approximately 19 weeks after the on-site). The country/territory should provide its comments and other relevant material in writing to the assessment team **at least 1 week** prior to any such meeting.
2. Subsequent to the receipt of the reviewers' comments and the face-to-face meeting, the assessment team will consider whether any further changes should be made to the draft MER and Executive Summary, and as necessary, revise the draft MER and Executive Summary. Where significant substantive changes are made to the MER after the face-to-face meeting, the Secretariat should consider circulating a revised second draft to external reviewers for a targeted review, if the timetable allows this.

Rule 18 – The Plenary Discussion

Identifying Issues for Plenary Discussion

1. The secretariat will send the revised Executive Summary and MER (3rd draft) to all delegations, observers and reviewers, including FATF (for circulation to FATF members) at least **5 weeks** prior to Plenary together with the conclusions of the internal quality and consistency review, and assessors' response. There should be no further changes to the substance of the draft MER thereafter before the discussion at the Working Group on Evaluations (WGE) and the Plenary. Delegations, observers and scientific experts will have **2 weeks** to provide any written comments on the MER and Executive Summary, and in particular, to identify any specific issues that they wish to discuss in Plenary. The comments should focus on the key substantive issues, or on other high level or horizontal aspects of the assessment, though other observations may also be made. The comments received will be made available to all delegations and observers.
2. Based on the MER and Executive Summary, and comments received, ideally three weeks preceding the Plenary, the secretariat will engage the country/territory, the assessment team, the reviewers and the WGE co-chairs, and prepare a list of (usually 5 to 7) priority and substantive issues that will be discussed in Plenary and or Working Group. This should take into account the issues that the assessed country/territory and delegations are most keen to discuss. The list of priority issues for discussion in Plenary would include key issues arising from the report (whether referenced by the country/territory, the assessment team or delegations) should focus on effectiveness, but may include issues related to technical compliance and the assessed country's risk and context, as well as any areas of inconsistency or interpretation with other MERs adopted by the FATF and/or MONEYVAL.
3. The secretariat will circulate a finalised list of priority issues to delegations and observers **at the latest 2 weeks** before the Plenary discussions. Drafting amendments received on the Executive Summary or MER can be made after the Plenary discussion, and should reflect the decisions made by Plenary. After discussion in the WGE, whose rules of procedures are regulated in Appendix 5 to this document, a revised key issue document is submitted to the Plenary for discussions.

Plenary Discussion

4. The discussion of each MER and Executive Summary (particularly the list of priority issues)[208] will focus on high level and key substantive issues, primarily concerning implementation in practice and effectiveness. Where appropriate, important technical issues would also be discussed. Adequate time should always be set aside to discuss the country/territory's response to the mutual evaluation and other issues. The discussion is likely, on average to take **3 to 4 hours** of Plenary time, though, where justified, it may be extended to maximum **1 day**. The procedure for the discussion will be as follows:

   a) The Secretariat briefly presents in high level terms the key issues and findings from the report. The team will have the opportunity to intervene/comment on any issue concerning the Executive Summary or MER.
   b) Assessed country/territory makes a short opening statement.
   c) The Plenary discusses the list of priority issues identified. This would usually be introduced briefly by WGE co-chairs.
   d) Adequate time will be set aside to discuss the overall situation of the assessed country/territory's AML/CFT regime and ML/TF risks, the priority actions set out in the Executive Summary, the country/territory's response to the mutual evaluation including any actions already taken, and the key findings.
   e) Time permitting, other issues could be raised from the floor, and discussed by the Plenary.

Rule 19 – Adoption of the MER and Executive Summary

(a) Finalisation of the MER and Executive Summary for Plenary adoption

1. At the Plenary the representatives of the FATF and MONEYVAL Secretariats and Scientific Experts will be expected to assist and advise on all issues relating to the interpretation of the Recommendations, and the quality and consistency aspects of the draft MERs. The Plenary discussion will provide members and observers adequate opportunity to raise and discuss concerns about the quality and consistency of an MER. At the end of the Plenary discussion, the MER and the Executive Summary will be submitted to Plenary for adoption. The adopted report will be subject to further checks for typographical or similar errors.

2. Where substantive changes are required to be made to the draft report, either because additional information is required to be added, or the report has to be substantially amended, then the Plenary could decide to defer adoption of the report, and agree to have a further discussion of an amended report at the following Plenary.

3. The assessment team would be responsible for ensuring that all the changes agreed by the Plenary had been made. Following the discussion of the report, and prior to its formal adoption, the Plenary should discuss the nature of the follow-up measures or other procedures that would be required.

4. The final report is a report of the Council of Europe/MONEYVAL, and not a report by the assessors. As such, the Plenary will retain the final decision on the wording of any report, consistent with the requirements of the Standards and Methodology. The Plenary will give careful consideration to the views of the assessors and the country/territory when deciding on the wording, as well as take into account the need to ensure consistency between reports.

5. Following the discussion of the report at the Plenary meeting, the secretariat will amend all documents as necessary, and will circulate a revised version of the report to the country/territory **within 1 week of the Plenary**. Care will be taken to ensure that no confidential information is included in the report. **Within 2 weeks of receipt** of the final

[208] The Executive Summary will describe the key risks, the strengths and weaknesses of the system, and the priority actions for the country to improve its AML/CFT regime.

version of the MER from the secretariat, the Head of delegation must confirm that the MER is accurate and/or advise of any typographical or similar errors in the MER.

(b) Review of major quality and consistency problems by the AML/CFT global network

6. All finalised MERs adopted by MONEYVAL shall be sent by the secretariat, prior to their formal publication on MONEYVAL's website, to the FATF Secretariat for circulation the global AML/CFT network. The FATF or FSRBs members or secretariats, or the IFIs shall have **2 weeks** to advise the FATF secretariat in writing if they have any serious concerns about the quality and consistency of the MER/FUR and if so, to indicate their specific concerns and how these concerns meet the substantive threshold.[209] This process shall be governed by the FATF procedures related to the ex-post facto Global Quality and Consistency Review. In such cases, MONEYVAL, the assessment team and the assessed country/territory will be invited to provide input in the process.

7. MONEYVAL shall consider the recommendations made by the FATF on the appropriate action that could be taken as well as any other measures that may be requested by the FATF as a result of this process and decide on the appropriate course of action. This may involve that the report is reconsidered and/or changes be made before any publication. In such cases, re-opening of discussions or changes to the report shall cover only the identified quality and consistency aspects.

8. The Executive Summary and MER shall not be made public until the issue is resolved within MONEYVAL's and FATF's respective processes.

(c) Communication of the adopted report and publication

9. The MER shall be published **within 6 weeks** of adoption, after having passed the quality and consistency review of the global AML/CFT network. The country/territory assessed shall provide, in view of its publication on MONEYVAL's website, a translation of the Executive Summary into the country's official language(s). According to the Council of Europe publication policy, the full MER shall be translated (where appropriate) into the relevant working languages of the Organisation and published soon after.

10. The final report shall be formally transmitted to the Permanent Representation of the country/territory concerned. A copy of the report shall also be transmitted formally to relevant organs, bodies and committees of the Council of Europe.

TITLE III. FOLLOW-UP PROCEDURES FOR MONITORING PROGRESS AS A RESULT OF THE MUTUAL EVALUATION

Rule 20 – Follow-up processes as a result of the fourth evaluation rounds

1. The rules set out under MONEYVAL's Rules of Procedure for the 4th round of mutual evaluations with respect to monitoring progress as a result of mutual evaluation procedures (i.e. Rules 12 and 13) shall continue to be applicable to States and territories subject to MONEYVAL's processes until otherwise decided by the MONEYVAL Plenary.

Rule 21 – General principles for follow-up processes under the fifth evaluation round

1. The follow-up process is intended to:

   (i) contribute to improving states and territories' implementation of the Standards within a reasonable timeframe;

[209] The substantive threshold is when serious or major issues of quality and consistency are identified, with the potential to affect the credibility of the FATF and MONEYVAL brand as a whole.

(ii) provide regular monitoring and up-to-date information on countries' compliance with the Standards (including the effectiveness of their AML/CFT systems);

(iii) apply sufficient peer pressure and accountability; and

(iv) better align the FATF and FSAP assessment cycle.

2. Following the discussion and adoption of a MER, the country/territory could be placed in either regular or enhanced follow-up:

   a) Regular follow-up is the default monitoring mechanism for all countries.

   b) Enhanced follow-up involves a more intensive process of follow-up. This is intended to be a targeted but more comprehensive report on the countries/territories' progress, with the main focus being on areas in which there have been changes, high risk areas identified in the MER or subsequently and on the priority areas for action.

3. MONEYVAL's follow-up processes shall take into account, as appropriate, other complementary processes designed to ensure compliance. These may include for instance its own Compliance Enhancing Procedures or action taken by the FATF (and relevant working groups), or in the case of joint members, any relevant reports submitted by that member to relevant bodies of the global AML/CFT process. This shall be ensured by taking into account any relevant reviews and monitoring reports under the above-mentioned processes, as appropriate. If a different conclusion is reached from previous MONEYVAL reports in cases where the standards and the relevant aspects of the country/territory's AML/CFT regime have not changed, the reasons basing this conclusion shall be set out in the relevant analysis.

4. In preparation for the follow-up reports, the country will provide an update to the Secretariat setting out the actions it has taken or is taking to address the priority actions and recommendations, and deficiencies in its MER. The country shall submit information regarding technical compliance (which may be used to justify re-ratings) and effectiveness (for information only). Updates on effectiveness facilitate a better understanding by MONEYVAL of the progress made over time.

5. Effectiveness updates should include any information that goes towards addressing the priority actions or recommendations in the MER, such as the lists in the FATF Methodology on the Examples of Information that could support the conclusions on Core Issues for each Immediate Outcome.

6. All reports are subject to peer review by MONEYVAL delegations, a Rapporteur Team, and the secretariat, which should highlight the progress made and the remaining deficiencies and propose timelines to take remedial actions. The Rapporteur Team shall be formed by at least 2 countries/territories appointed at the previous plenary or formed by the Bureau between Plenary sessions and include 2 to 6 experts from these delegations.

7. The process for follow-up reports is set out below[210]:

   a) The country/territory seeking a technical compliance re-rating should indicate on which Recommendations a re-rating will be requested, 7 months in advance of Plenary meetings. The country/territory shall provide its report, based on the templates agreed by MONEYVAL for this purpose, **at least 6 months** before the update report is due to be discussed by MONEYVAL; the Plenary will take into account relevant laws, regulations or other AML/CFT measures that are in force and effect at that time[211].

[210] For follow-up reports considered by MONEYVAL via written procedure, a specific timetable for preparation and adoption for the respective FUR shall be approved by MONEYVAL prior to the start of the review process. This timetable shall respect the minimum deadlines set out in this Rule.

[211] This rule may only be relaxed in the exceptional case where the legislation is not yet in force at the six-month deadline, but the text will not change and will be in force by the time of the Plenary. In other words, the legislation has been enacted, but is awaiting the expiry of an implementation or transitional period before it is enforceable. In all other

b) The report will be circulated upon receipt to the Rapporteur Team appointed at the previous plenary to review the report;

c) The Heads of Delegation of the countries/territories appointed to form the Rapporteur team will assign scrutiny of the relevant parts of the report among their delegation for review. They shall seek to involve former mutual evaluation team members, experienced assessors or otherwise regular members of their delegation. The Rapporteur Team shall prepare a desk-based review which shall form the basis for the summary report to the Plenary. The desk-based review will be sent to the secretariat **at least 11 weeks** before the update report is due to be discussed by MONEYVAL;

d) The summary report, based on the desk-based review, shall include an independent analysis of the secretariat on selected aspects. The summary report shall follow the standardised format set out in Appendix 6. The summary report will be sent to the State/territory for comments **at least 9 weeks** before the Plenary discussion. The country/territory will have **2 weeks** to provide comments to the secretariat.

e) Follow-up reports with technical compliance re-ratings should be circulated to all members, associate members and observers, including FATF (for circulation to members of the Global Network), at least 5 weeks prior to discussion in the relevant plenary meeting, who have 2 weeks to provide written comments on such reports. Rapporteur teams and secretariat (where necessary, consulting with WGE co-chairs and/or scientific experts) should compile a short list of the most significant issues, and should circulate this to all members, observers and associate members at least 2 weeks prior to the relevant plenary discussion. The relevant plenary discussion should prioritise discussion of these issues and should be limited in time and scope.

f) The reporting country/territory shall be given the opportunity to briefly present its report. The secretariat shall present its analysis as well as the proposed recommendation regarding the next steps in the follow-up process. MONEYVAL shall discuss as a matter of priority the identified substantive issues. Delegations and observers, including the Rapporteur team, may raise any additional questions aimed at seeking clarifications about the information provided in the report.

8. Countries may seek re-ratings for technical compliance as part of the follow-up process with recommendations rated as NC or PC. The decision on re-ratings shall be taken by the Plenary. Re-ratings may be allowed if the follow-up report, and other relevant information submitted by the country, provides sufficient justification for the Plenary to come to such a conclusion, based on an analysis conducted by the Secretariat. Re-rating requests will not be considered where the Secretariat/the Rapporteur Teams determine(s) that the legal, institutional or operational framework has not changed since the country's/territory's MER (or previous FUR, if applicable) and there have been no changes to the FATF Standards or their interpretation.[212] The general expectation[213] is for countries to have addressed most if not all of the technical compliance deficiencies by the end of the 3rd year after the adoption of the MER. The analysis of the follow-up report where re-ratings for technical compliance are requested shall be conducted in accordance with the process set out in Appendix 7. If any of the FATF standards have been revised since the end of the on-site visit (or previous FUR, if applicable), the country will be assessed for compliance with all revised standards at the time

cases, the procedural deadlines should be strictly followed to ensure that experts have sufficient time to do their analysis.

[212] The determination as to whether the re-rating request is in line with these criteria shall be made upon initial circulation of the report to the rapporteur team. Where there is disagreement between the expert(s) and the assessed country in this respect, they should discuss with scientific experts to achieve an agreement.

[213] It is up to the Plenary to determine the extent to which its members are subject to this general expectation, depending on the member's context.

its re-rating request is considered (including cases where the revised Recommendation was rated LC or C).

9. The plenary may consider excluding the discussion of an individual criterion rating unless it will have an impact on the overall Recommendation rating. By separate decision, the plenary may also opt to approve follow-up reports through written process.[214]

10. In the exceptional case that it comes to the Plenary's attention that a country has significantly lowered its compliance with the FATF standards, the Plenary may request the country to address any new deficiencies as part of the follow-up process.

11. If any of the FATF standards have been revised since the last day of the on-site visit, the country will be assessed for compliance with all revised standards at the time its re-rating request is considered.

12. For countries subject to review by the International Cooperation Review Group (on the basis of an agreed ICRG action plan), no reporting is expected on the Recommendations that are included in an ongoing ICRG action plan. However, overall progress on each Recommendation is still expected to be achieved, including on parts of Recommendations that are not covered by the ICRG action plan, under the normal timelines, or as soon as the country has completed its ICRG action plan (if this is after the regular timelines).

13. Following the publication of a MER, and following any Plenary decision related to follow-up taken, the Head of delegation of the country/territory concerned shall be formally notified about the decision of the Plenary regarding the follow-up procedures and the reporting timelines.

14. The general publication policy of FATF and MONEYVAL applies to actions taken under the follow-up policy. Regular follow-up reports and their analysis will be published. The Plenary will retain flexibility on the frequency with which enhanced follow-up reports are published, but they will be published whenever there is a re-rating.

15. After adoption, and prior to publication, final follow-up reports with TC re-ratings should be provided to the FATF Secretariat and all other assessment bodies for consideration in the post-Plenary Quality and Consistency Review process described in the Post-Plenary Quality and Consistency Review section of these Procedures. Follow-up reports where no issues are raised through the pre-plenary review process or during the plenary discussion are not subject to this post – Plenary Q&C review process.

Rule 22 – Regular Follow-up

Regular follow-up will be the default mechanism to ensure a continuous and on-going system of monitoring. This is the minimum standard that will apply to all members after 2-and-a-half years from the adoption of the country's MER and subsequently at 3-year intervals.

Rule 23 – Enhanced Follow-up

1. The Plenary may decide, at its discretion, that the country should be placed in enhanced follow-up, which would result in the country reporting back more frequently than for regular follow-up. Countries in enhanced follow-up would typically first report back to the Plenary two years after the adoption of the country's MER, and subsequently report twice more at yearly intervals, unless the Plenary decides otherwise. The Plenary retains the discretion to vary the specific frequency of reporting.

[214] In this case, at a minimum, if comments are raised when a report is circulated for approval by written process, the Secretariat should work with the Rapporteur teams and the assessed country/territory to amend the report and address comments received. The report would be then circulated again for approval and be discussed in Plenary if any other comments are raised.

2. In deciding whether to place a country/territory in enhanced follow-up, the Plenary would consider the following factors:

   a) After the discussion of the MER: a country/territory will be placed immediately into enhanced follow-up if any one of the following applies:

      (i) it has 8 or more NC/PC ratings for technical compliance, or

      (ii) it is rated NC/PC on any one or more of R.3, 5, 10, 11 and 20, or

      (iii) it has a low or moderate level of effectiveness for 7 or more of the 11 effectiveness outcomes, or

      (iv) it has a low level of effectiveness for 4 or more of the 11 effectiveness outcomes.

   b) After the discussion of a follow-up report: the Plenary could decide to place the country/territory into enhanced follow-up at any stage in the regular follow-up process, if a significant number of priority actions have not been adequately addressed on a timely basis. A country would also be placed into enhanced follow-up if, during the regular follow-up process, its level of technical compliance changed to a level that the Plenary considers as equivalent to NC/PC on any one or more of R.3, 5, 10, 11 and 20.

3. In addition to more frequent reporting, the Plenary may also apply other compliance measures to countries and territories as set out in Title IV.

4. The Plenary may also decide to move the country/territory back to regular reporting at any time during the enhanced follow-up process when the country/territory entered enhanced follow-up on the basis of meeting a criterion in paragraph 23(2(a(i,ii))), the Plenary may decide that the country/territory may be moved from enhanced to regular follow-up following Plenary's decision that the country/territory no longer meets those criteria. At that time the Plenary will decide the timing of the country/territory's next regular follow-up report. The criteria for being placed under or exiting from enhanced follow-up at any stage of the follow-up process after the adoption of the MER will be primarily based on a qualitative analysis of the level of progress made against priority recommended actions in the MER as well as the level of technical compliance and effectiveness.

Rule 24 – MER Follow-up Assessment

Deleted

TITLE IV. COMPLIANCE ENHANCING PROCEDURES

Rule 25 – General principles

1. MONEYVAL may take action at any time in respect of countries and territories subject to its evaluation procedures for failure to implement the reference documents or the recommendations in mutual evaluation reports. It should be guided by the following principles:

   a) flexibility in order to deal with situations which require urgent action by the Plenary when issues of non-compliance arise;

   b) equality of treatment for MONEYVAL countries/territories;

   c) a graduated approach for dealing with non-complying countries/territories;

   d) approval by the Plenary of the steps to be taken, whilst allowing for some discretion regarding their application.

2. There are several ways by which a country/territory could come to the attention of MONEYVAL for the purpose of application of Compliance Enhancing Procedures (CEPs):

a) as a result of MONEYVAL's evaluation processes; or

b) as a result of a Bureau's decision to refer to MONEYVAL a serious issue of concern[215] which could qualify for the application of Compliance Enhancing Procedures.

3. Any MONEYVAL delegation, through their Head of delegation, can also bring to the attention of MONEYVAL a serious issue which could qualify for the application of Compliance Enhancing Procedures, by outlining in writing its concerns and the nature of the difficulties encountered. When such a notification is received, the Bureau shall gather any further additional clarifications it may require before discussing its merits, by liaising, as appropriate, with the MONEYVAL delegation and the country or territory concerned and taking a decision to present this issue for Plenary decision.

4. In cases when MONEYVAL has identified the need to take action, the Chairman of MONEYVAL shall send a letter to the Head of Delegation concerned, with a copy to MONEYVAL delegations and the Permanent Representative of the Country/territory to the Council of Europe, drawing his/her attention to non-compliance with the reference documents and requiring the Country or territory concerned to provide a report before the next MONEYVAL plenary meeting (or regular reports) within a fixed timeframe, so as to assess the extent of the problem and any actions or progress of the country/territory concerned in addressing the issues of concern and implementing the reference documents.

Rule 26 – Compliance steps

1. In addition to reporting, MONEYVAL may also apply other steps to a non-complying country/territory, as follows:

   Step 1: MONEYVAL inviting the Secretary General of the Council of Europe to send a letter to the relevant Minister(s) of the country or territory concerned, drawing his/her/their attention to non-compliance with the reference documents and the necessary corrective measures to be taken;

   Step 2: Arranging a high-level mission to the non-complying country or territory to meet relevant Ministers and senior officials to reinforce this message;

   Step 3: In the context of the application of the 2012 FATF Recommendation 19 by MONEYVAL countries and territories, issuing a formal public statement to the effect that a country or territory insufficiently complied with the reference documents and inviting the members of the global AML/CFT network to take into account the risks posed by the noncomplying country or territory.

   Step 4: Referring the matter for possible consideration under the FATF's International Cooperation Review Group (ICRG) process, if this meets the nomination criteria set out under the ICRG procedures.

2. In all cases, the Chairman can require the country or territory to provide regular reports to the MONEYVAL Bureau and Plenary on progress in addressing the issues of concern.

3. Notwithstanding a reference to the FATF's ICRG under step 4, the MONEYVAL Plenary retains its decision-making powers under the CEPs on any necessary measures that need applying, in order to assist the country/territory to meet the requirements for removal from these procedures.

Rule 27 – Practical modalities, decision making and lifting of CEPs

[215] Such issues may include for example situations where a) there is a demonstrated unwillingness or inability to respond adequately to requests, *b)* where non-compliance with certain Recommendations results in serious vulnerabilities in the AML/CFT framework c*)* where there are substantial ML or FT threats or risks d) if substantial changes occur in a State/territory at a time when this cannot be addressed by the formal follow-up.

1. As regards the application of steps 1 and 2, the practical modalities are as follows: the Chairman would propose to the Plenary, after consultation with the Bureau, the steps which in his/her estimation should be taken in relation to the non-complying country or territory. The Plenary would then decide the parameters for action, and the Chairman would be authorised to take action, where necessary through the secretariat, within these limits.

2. If after a reasonable time the country or territory in question persists in its failure to comply significantly with the reference documents and the recommendations, efforts would need to be intensified. These will involve the application of step 3 and 4, either separately or cumulatively. The Chairman, through the MONEYVAL/Council of Europe Secretariat, may bring the matter to the attention of the Committee of Ministers of the Council of Europe. The Chairman would also be authorised at this juncture to propose to the Plenary that step(s) 3 and/or 4 be taken, and to pursue the action approved by the Plenary . The Chairman would have no discretion to modify or deviate from the course of conduct approved by the Plenary. The Chairman, through the MONEYVAL/Council of Europe Secretariat, shall inform the Committee of Ministers about any action taken under these steps.

3. A written analysis shall be prepared by the secretariat on the basis of the information provided by the non-complying country or territory and of any other reliable sources of information, outlining the main areas of concern, the action taken by the non-complying country or territory and a recommendation regarding the next step(s) in the compliance enhancing procedures. The report submitted by the non-complying Country or territory together with the secretariat analysis shall be reviewed by the Bureau. When appropriate or feasible, the Bureau may request to hold an exchange of views with the non-complying Country or territory before a CEP report , analysis and recommendations are discussed by the Plenary.

4. The **procedure** for discussing compliance enhancing reports is as follows:

   a) The secretariat shall briefly present the status of the application of CEPs in respect of the non-complying country or territory, outlining the key issues of concern and the findings of its analysis.

   b) The non-complying country or territory shall present the measures taken as a result of the CEPs and its views on its compliance with the reference documents.

   c) The Plenary shall discuss the issues of concern identified, whether the action taken (if any) may be considered as addressing in an adequate manner MONEYVAL's concerns and the extent of or speed of progress to rectify the issues of concern.

5. MONEYVAL shall decide at each Plenary meeting where a compliance enhancing report is being examined whether the country or territory concerned has taken adequate corrective action to address the issue(s) of concern in a timely manner, on the basis of the report submitted by the non-complying country or territory, as well as any other supporting documents, and whether any additional steps under the CEPs should be applied.

6. When considering compliance enhancing reports, MONEYVAL shall adopt the secretariat analysis and decide upon the appropriate step (s) under the CEPs which shall be applied, given the urgency and/or gravity of the issue(s) of concern. The adopted secretariat analysis of a CEP report and the report submitted by the non-complying Country or territory shall be published in accordance with MONEYVAL's publication rules.

7. When a country/territory is placed in compliance enhancing procedures, removal will be possible only when the issues of concern have been adequately addressed and that any technical deficiency has been addressed through legislation or other enforceable means, as appropriate. The latter should be in force and effect before a decision is taken to remove a country/territory from CEPs. Where necessary, there should also be evidence which satisfies

the plenary that there is effective implementation on the issues which caused the imposition of CEPS. This may, but need not necessarily require, a brief on-site mission.

TITLE V. PROCEDURES FOR ACTION IN EXCEPTIONAL CIRCUMSTANCES

Rule 28 – Action in exceptional circumstances

1. In exceptional cases, where there are urgent and serious concerns, and where a prompt (re)action by MONEYVAL is required, the Chairman shall be permitted to undertake a course of action, as set out in the paragraphs below, as an interim measure until MONEYVAL can be fully seized of the problem at its earliest Plenary meeting and take an informed decision with a view to resolving it. This mechanism, which shall be used only in exceptional circumstances, is aimed at providing a framework for a rapid reaction to situations which may involve important issues for MONEYVAL/Council of Europe or any of its States and territories.
2. In determining whether the matter requires immediate action and cannot wait until a Plenary meeting is held, the Chairman shall consult with the Bureau and the Executive Secretary of MONEYVAL. When doing so, all Parties shall consider in particular a) the seriousness of the situation, b) the level of urgency, and any likely adverse consequences of inaction by MONEYVAL/Council of Europe. The Chairman and/or the Executive Secretary shall engage in this process as appropriate with the MONEYVAL Country or territory concerned and interested parties.
3. Action taken under this mechanism may involve as appropriate an on-site mission, face-to-face or teleconference meeting(s) with the Country or territory concerned and/or relevant representatives, a written analysis and/or expertise commissioned, or any other appropriate measure the Bureau may consider appropriate.
4. Upon initiation of the course of action, the Chairman shall notify all MONEYVAL delegations. A report shall be presented to MONEYVAL, at its next meeting, about the situation and the developments resulting from the course of action undertaken, together with any recommendations on measures that MONEYVAL should consider at that time, including further monitoring by MONEYVAL.
5. Any further action shall be discussed and decided by MONEYVAL at its earliest Plenary, applying, where appropriate, its Rules of Procedure.
6. A MONEYVAL member state or territory is also entitled to nominate any jurisdiction to the ICRG in accordance with the ICRG Procedures and Guidelines. The nomination document shall be addressed to the ICRG co-chairs and forwarded by the Head of the MONEYVAL Member Delegation to the FATF Secretariat through the MONEYVAL Secretariat. MONEYVAL and its Secretariat shall not bear any responsibility for any aspect of such a nomination. The MONEYVAL Secretariat will not assess the content of the nomination, nor whether the nominating country has provided all the necessary assessments and justifications for ICRG purposes.

Rule 28 bis – MONEYVAL working methods in exceptional circumstances

1. In exceptional circumstances, MONEYVAL may adjust its working methods by substituting physical meetings and activities described in these Rules of Procedure for virtual meetings and activities with the use of videoconference facilities, including so called ‘hybrid’ meetings allowing for both physical and virtual participation of delegations.
2. The Chair upon consultation with the Bureau shall take a decision on which meetings and activities of MONEYVAL may be held virtually or in a ‘hybrid’ fashion.
3. In cases where meetings and activities take place virtually or in a ‘hybrid’ fashion, they are to be held in full accordance with these Rules of Procedure.

4. In the course of a virtual or 'hybrid' Plenary discussion, the Plenary may refrain from taking a decision on a given item and opt for a written ('silent') procedure in accordance with Rule 6, paragraph 6 of these Rules of Procedure."

TITLE VI. CONFIDENTIALITY

Rule 29 – The principle of confidentiality

1. Information gathered by MONEYVAL in relation to an evaluation, follow-up or compliance procedure, including replies to the questionnaires, and related correspondence shall be confidential.
2. All documents and information elaborated: (a) by an evaluated country/territory during a mutual evaluation exercise; (b) by the MONEYVAL secretariat or evaluators and (c) in the context of the consultation or review mechanisms, should be treated as confidential. These documents shall be used for the specific purpose provided. Such documents cannot be made public without a Committee decision based on a specific request to that effect.
3. This confidentiality requirement does not apply to documents and information of an assessed country/territory if the originator of the document consents to their release or if these have been made already public by the country/territory concerned.
4. The key findings provided by the assessment team to the assessed country/territory officials at the closing meeting and the draft evaluation reports are confidential. With the permission of the country/territory undergoing evaluation, such documents may be passed by the secretariat to the IMF or World Bank, if it is required to assist with an FSAP mission planned or in progress.
5. A country/territory evaluated by the IMF or World Bank on behalf of MONEYVAL shall be bound by the confidentiality requirements of the evaluation process as set out under the procedures of these international financial institutions. However, when a country/territory accepts to be evaluated under these procedures and following the Plenary's approval for this evaluation to be undertaken by another organisation, it shall expressly agree to provide to MONEYVAL, through its secretariat, a copy of all documents and information/communications shared between the country/territory and the assessment body for the purpose of the evaluation.
6. No personal data shall be published without the express consent of the person concerned.

Rule 30 – Obligation to maintain confidentiality

1. Representatives of MONEYVAL delegations from countries/territories, from observer States, organisations, institutions and bodies, scientific experts, experts and other persons assisting the Committee are required to maintain the confidentiality of the facts or information of which they have become aware during the exercise of their functions, during and after their mandate.
2. These confidentiality requirements apply equally to the secretariat and any other person or delegation with access to MONEYVAL's documents or information. The members of the assessment team and reviewers shall sign a confidentiality agreement before becoming involved in the evaluation process.

Rule 31 – Violation of confidentiality

1. If there are serious grounds for believing that any of the persons covered under the present Title has violated the obligation of confidentiality, MONEYVAL may, after the person concerned has had an opportunity to state his or her view to the Bureau, decide to inform the Secretary General of the Council of Europe, and/or the Permanent Representation of the

country concerned to the Council of Europe, and/or the Organisation/body concerned and request that appropriate measures be taken, including removing the representative from participating to MONEYVAL activities.

TITLE VII. PUBLICATION POLICY

Rule 32 – General publication principles

1. As set out in article 5(13) of MONEYVAL's statute, all reports adopted by MONEYVAL shall be public. The public website shall include up to date information on the status of the country/territory in the evaluation process, and if applicable, on the next steps. These principles apply to MONEYVAL's activities as well as any action under MONEYVAL's evaluation procedures.

TITLE VIII. FINAL CLAUSES

Rule 33 – Amendments

1. Any Head of delegation of a country/territory with the right to vote, the Chairman or the Executive Secretary may, at any time, propose an amendment to these Rules. A proposal to that effect shall be submitted in writing to the Bureau. It shall be for the Bureau to decide whether or not this proposal is submitted to MONEYVAL.
2. If the Bureau decides not to submit the proposal to MONEYVAL, it shall be included on the agenda of MONEYVAL only if it receives the support of one fourth of the MONEYVAL delegations with a right to vote at any given moment.
3. MONEYVAL may adopt an amendment suggested by a majority of the votes cast.

Rule 34 – Entry into force of the Rules

The present rules entered into force on 8 December 2014.

TITLE IX. APPENDICES

Appendix 1 – Authorities and Businesses Typically Involved for On-Site Visit

MINISTRIES:

- Ministry of Finance.
- Ministry of Justice, including central authorities for international co-operation.
- Ministry of Interior.
- Ministry of Foreign Affairs.
- Ministry responsible for the law relating to legal persons, legal arrangements, and non-profit organisations.
- Other bodies or committees to co-ordinate AML/CFT action, including the assessment of the money laundering and terrorist financing risks at the national level.

CRIMINAL JUSTICE AND OPERATIONAL AGENCIES:

- The FIU.
- Law enforcement agencies including police and other relevant investigative bodies.
- Prosecution authorities including any specialised confiscation agencies.
- Customs service, border agencies, and where relevant, trade promotion and investment agencies.
- If relevant - specialised drug or anti-corruption agencies, tax authorities, intelligence or security services.
- Task forces or commissions on ML, FT or organised crime.

FINANCIAL SECTOR BODIES:

- Ministries/agencies responsible for licensing, registering or otherwise authorising financial institutions.
- Supervisors of financial institutions, including the supervisors for banking and other credit institutions, insurance, and securities and investment.
- Supervisors or authorities responsible for monitoring and ensuring AML/CFT compliance by other types of financial institutions, in particular bureaux de change and money remittance businesses.
- Exchanges for securities, futures and other traded instruments.
- If relevant, Central Bank.
- The relevant financial sector associations, and a representative sample of financial institutions (including both senior executives and compliance officers, and where appropriate internal auditors).
- A representative sample of external auditors.

DNFBP AND OTHER MATTERS:

- Casino supervisory body;
- Supervisor or other authority or Self-Regulatory Body (SRB) responsible for monitoring AML/CFT compliance by other DNFBPs;
- Registry for companies and other legal persons, and for legal arrangements (if applicable);
- Bodies or mechanisms that have oversight of non-profit organisations, for example tax authorities (where relevant);
- A representative sample of professionals involved in non-financial businesses and professions (managers or persons in charge of AML/CFT matters (e.g. compliance officers) in casinos, real estate agencies, precious metals/stones businesses as well as lawyers, notaries, accountants and any person providing trust and company services);
- Any other agencies or bodies that may be relevant (e.g. reputable academics relating to AML/CFT and civil societies).

Efficient use has to be made of the time available on-site, and it is therefore suggested that the meetings with the financial sector and DNFBP associations also have the representative sample of institutions/DNFBP present.

Appendix 2 – Terms of reference of MONEYVAL's Ad Hoc Group of experts

Terms of Reference

Purpose

An Ad Hoc Group of experts will be established for each mutual evaluation to assist the assessors, the plenary, the Chairman and secretariat in the mutual evaluation process and act as a reviewer. Each Ad-hoc group shall contain at least one external reviewer.

The secretariat shall assist each Ad Hoc Group of experts to undertake its tasks.

Participation

The Ad Hoc Group of Experts will be composed of qualified volunteer experts, based on their professional experience, demonstrated expertise as assessors and their knowledge of the AML/CFT specificities. A pool would be maintained and kept up to date, including experts from MONEYVAL, FATF, IFIs, other FSRBs (including their secretariat members), based on nomination proposals.

Role and function

The primary functions of the Ad Hoc Group of experts are to ensure MERs are of an acceptable level of quality and consistency, and to assist the assessment team and the assessed country by reviewing and providing timely input on the scoping note and the draft MER and Executive Summary (including any annexes) with a view to:

a) Commenting on assessors' proposals for the scope of the on-site, including on whether the assessors' draft scoping note reflects a reasonable view on the focus of the assessment.

b) Reflecting a correct interpretation of the FATF standards and application of the methodology (including the assessment of risks, integration of the findings on technical compliance and effectiveness, and areas where the analysis and conclusions are identified as being clearly deficient).

c) Checking whether the description and analysis supports the conclusions (including ratings), and whether, based on these findings, sensible recommended actions and priority actions for improvement are made.

d) Where applicable, highlighting potential inconsistencies with earlier decisions adopted by the FATF and/or MONEYVAL on technical compliance and effectiveness issues, and that horizontal (cross-cutting issues) are adequately addressed.

e) Checking that the substance of the report is generally coherent and comprehensible.

In addition, on the basis of reciprocity, experienced experts from the pool may also be called upon to contribute as MONEYVAL reviewers to an FATF or FSRB mutual evaluation process.

The objective of the Ad Hoc Group is to identify and highlight what appear to them to be problematic issues in each sector of a draft report, which may impact on the quality and/or consistency of the assessment overall compared with other adopted reports, or on the interpretation of the relevant international standards in the draft report. The ad hoc group of experts will undertake any assignments as set out in MONEYVAL's rules of procedure and advise as requested in writing within the agreed timescales, as appropriate, the Chairman, secretariat and examiners. It may be assisted in its mandate by MONEYVAL's scientific experts, through the secretariat.

The Ad Hoc Group of experts will primarily perform its functions and responsibilities primarily on line between plenary meetings, though meetings may be organised if necessary.

Modalities

Proposals for the pool from which the ad-hoc groups will be formed for each report should be submitted to the secretariat. The composition of the pool as a whole will be kept under regular

review by the Plenary. The composition of specific ad-hoc groups for each report will be communicated to the assessed country/territory no less than 4 months before the on-site visit and to the Plenary as soon as it is practicable.

Appendix 3 – Terms of reference of MONEYVAL's Advisory Group on Policy and Evaluation

Deleted

Appendix 4 – Terms of reference of MONEYVAL's Working Group on Evaluations

Terms of Reference

Purpose

The Working Group on Evaluations (WGE) is established to assist MONEYVAL by preparing the plenary discussion and proposing solutions to the Plenary on technical and some other significant issues, in order to allow the plenary to focus discussions on primarily effectiveness issues, matters of substance and recommendations to the assessed jurisdiction. The discussions conducted at the WGE are expected to guide the decisions of the Plenary in relation to priority and substantive issues. The WGE does not have decision-making powers which rest with the Plenary. The Plenary will take the final decisions on changes of a substantive nature to an MER.

Participation

Participation in the WGE is open to 1-3 representatives from each MONEYVAL country/territory and 1-3 representatives from each observer to MONEYVAL. Meetings of the WGE will also involve participation of members of the evaluation team, the assessed jurisdiction's delegation, reviewers, chairman of MONEYVAL and MONEYVAL scientific experts.

Term

The term of the WGE will continue until otherwise mandated by the Plenary.

Role and functions

The WGE will support the work of the MONEYVAL Plenary by:

1. Identifying and prioritising issues for MONEYVAL Plenary discussion of mutual evaluations and any related follow-up actions.
2. Discussing a list of issues, covering both technical compliance and effectiveness issues, including horizontal issues or questions of interpretation
3. Ensuring that the process applies a clear understanding of the FATF standards and that any areas of inconsistency or interpretation with other MERs adopted by the FATF or MONEYVAL are being discussed with a view to their correction by the Plenary and ensuring the quality and consistency of mutual evaluations.
4. Referring significant or horizontal interpretation issues of the FATF standards back to the Plenary to consider possible policy implications, with proposed solutions if possible.
5. Undertaking any other tasks as assigned to it by the Plenary.

The co-chairs will support the work of the WGE by:

1. Engaging with the Secretariat to prepare a list of priority and substantive issues for WGE discussion and a list of key issues for Plenary discussion;
2. Chairing WGE meetings;
3. Undertaking any other tasks as assigned to it by the Plenary;
4. Reporting to the Plenary on the progress in carrying out its work, as necessary.

Chairs

The group will be chaired by a MONEYVAL scientific expert and by an expert from a MONEYVAL country/territory, who would undertake their roles in independent capacities. Both experts should have a demonstrated and strong AML/CFT expertise. The chair(s) of the Group would be decided by the Bureau for a mandate of 2 years, renewable. The WGE co-chairs shall be guided by the Principles of conduct for MONEYVAL Bureau members, working group co-chairs and scientific experts.

Budgetary aspects

Participation of 1 nominated representative from each MONEYVAL country/territory to WGE meetings shall be covered from MONEYVAL's budget. Observers participate at the costs of the sending institution.

Appendix 5 – Rules of procedure of MONEYVAL's Working Group on Evaluations

Process before the meeting

1. According to paragraph 1 of Rule 18 of MONEYVAL's 5th Round Rules of Procedure, the secretariat is expected to circulate the 3rd (and final) draft of the Executive Summary and MER to all delegations, observers, scientific experts and reviewers 5 weeks prior to the plenary.

2. Delegations, observers, scientific experts and reviewers will have 2 weeks to provide any written comments on the MER and Executive Summary. The comments should focus on issues of substance, or on other high level or horizontal aspects of the assessment, though other observations may also be made.

3. Examples of issues of substance would include: (1) inconsistency between the analysis of an immediate outcome and the rating; (2) inconsistency in the treatment of similar issues in different reports; (3) issues of materiality and risk; (4) issues of a technical nature which could have a significant impact on the interpretation of a particular Recommendation; and (5) issues of a horizontal nature, e.g. the proportionality and dissuasiveness of sanctions, or concerning different types of ML convictions (e.g. autonomous ML, third-party ML, self-laundering).

4. Delegations, observers, scientific experts and reviewers are also encouraged to submit any comments related to specific text in the report or requests for clarification, which may not be substantive issues and may not have a bearing on the rating of an Immediate Outcome or a Recommendation but may ultimately result in an improved version of the MER. These comments will be considered by the assessment team. The assessed country/territory may also be asked to provide clarifications, where these are requested by a delegation.

5. 2 weeks before the Plenary session, the secretariat will engage the assessed country/territory, the assessment team and the co-chairs to select the key issues.

6. If necessary, a decision may be taken by the co-chairs to include a certain key issue which had not previously been raised in any of the comments received. This should, however, be restricted to those situations where there are issues of serious concern (particularly with regard to ratings) which have not been raised by any delegation. Additional key issues may also become apparent in the course of a discussion of another key issue during the WGE meeting.

7. Once the key issues are selected, the assessed country/territory and the assessment team will be invited to provide their views and comments in writing, which will be summarised in the draft key issues document.

8. The draft key issues document will be circulated to delegations 2 weeks before the WGE meeting.

Process during the meeting

9. The co-chairs will open the meeting and invite the secretariat to present a brief overview of the key findings of the MER.

10. The co-chairs and/or the secretariat will then present each key issue and invite the WGE party which had raised the issue as well as the assessed jurisdiction to provide its comments. The assessment team will be invited to express their views on the key issue. The co-chairs will then open the floor for comments from delegations, observers, scientific experts and reviewers.

11. The WGE may decide to change the description of the key issue (for example to narrow down the issue, describe it better or merge several issues) before forwarding it to the Plenary, depending on how the discussion of the key issue evolves during the meeting. If so, the assessors and the assessed country/territory will be afforded the opportunity to redraft their views.

12. Decisions on key issues shall be taken by consensus. The co-chairs will determine whether consensus has been reached.

Process after the meeting

13. The secretariat and the co-chairs will review the "key issues document" and circulate it to the Plenary at least 1 day before the day on which the report will be discussed in Plenary.

14. Based on the WGE discussion, the assessors and the secretariat may agree to amend the MER before the Plenary meeting. The redrafting does not involve the assessed country/territory. However, any

change is shown to the assessed country/territory before it is finalised for circulation, and a possibility is given to the assessed country/territory to comment on the amendments.

15. In the Plenary, the co-chairs will introduce each (revised) key issue, 1 by 1. They will summarise the discussion held in the WGE and present its findings and decisions. The Plenary discussion will then proceed as provided in Rule 18, paragraph 4 of MONEYVAL's 5th round Rules of Procedure.

Appendix 6 – STANDARDISED FOLLOW-UP REPORT PUBLICATION FORMAT (FOR PUBLICATION)

[COUNTRY NAME: NUMBER & TYPE (E.g. Regular or Enhanced) OF FOLLOW-UP REPORT]

I. INTRODUCTION

1. The mutual evaluation report (MER) of [country name] was adopted on [date]. This follow-up report analyses the progress of [country name] in addressing the technical compliance deficiencies identified in its MER. Re-ratings are given where sufficient progress has been made. This report also analyses progress made in implementing new requirements relating to FATF Recommendations which have changed since the MER was adopted: [list the relevant Recommendations if applicable]. Overall, the expectation is that countries will have addressed most if not all technical compliance deficiencies by the end of the third year from the adoption of their MER. This report does not address what progress [country name] has made to improve its effectiveness. Progress on improving effectiveness will be analysed as part of a later follow-up assessment and, if found to be sufficient, may result in re-ratings of Immediate Outcomes at that time.

II. FINDINGS OF THE MUTUAL EVALUATION REPORT

2. The MER rated[216] [country name] as follows for technical compliance [*table to be updated accordingly*]:

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

3. Given these results, [*country name*] was placed in [*enhanced/enhanced (expedited)/regular*] follow-up.[217] The assessment of *[country name]*'s request for technical compliance re-ratings and the preparation of this report was undertaken by the following [*experts/members of the Secretariat*]:

   - *[Expert/Secretariat name(s) and title(s).]*

4. Section III of this report summarises the progress made to improve technical compliance. Section IV sets out the conclusion and a table showing which Recommendations have been re-rated.

III. OVERVIEW OF PROGRESS TO IMPROVE TECHNICAL COMPLIANCE

5. This section summarises the progress made by [*country name*] to improve its technical compliance by:

   a) Addressing the technical compliance deficiencies identified in the MER, and

   b) Implementing new requirements where the FATF Recommendations have changed since the MER was adopted (R.5 and R.8 [*include others if relevant*]).

---

[216] There are 4 possible levels of technical compliance: compliant (C), largely compliant (LC), partially compliant (PC), and noncompliant (NC).

[217] Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up is based on the FATF's traditional policy that deals with members with significant deficiencies (for technical compliance or effectiveness) in their AML/CFT systems and involves a more intensive process of follow-up.

3.1. Progress to address technical compliance deficiencies identified in the MER

6. [*Country name*] has made progress to address the technical compliance deficiencies identified in the MER in relation to Recommendations: [*list all Recommendations rated NC which the country has requested a re-rating*] (which were rated NC); [*list all Recommendations rated PC which the country has requested a re-rating*] (which were rated PC). [*If the country has also sought upgrades on recommendations rated LC, this should be included here*.]

7. As a result of this progress, [*Country name*] has been re-rated on Recommendations: [*list relevant Recommendations*]. The FATF welcomes the steps that [*Country name*] has taken to improve its technical compliance with [*list relevant Recommendations*]; however, insufficient progress has been made to justify a re-rating of these Recommendations.

Recommendation [R.] (Originally rated [NC/PC/LC])

8. [*Summary of identified deficiency and progress taken to address it*]

9. [*Conclusion on Recommendation with proposal for rating*]

Recommendation [R.] (Originally rated [NC/PC/LC])

10. [*Summary of identified deficiency and progress taken to address it*]

11. [*Conclusion on Recommendation with proposal for rating*]

Recommendation [R.] (Originally rated [NC/PC/LC])

12. [*Summary of identified deficiency and progress taken to address it*]

13. [*Conclusion on Recommendation with proposal for rating*]

3.2. Progress on Recommendations which have changed since adoption of the MER

14.

Recommendation [R.] (Originally rated [NC/PC/LC/C])

15. [*Summary of change to Rec and progress made to implement it.]*

16. [Conclusion *on Recommendation with proposal for rating*]

IV. CONCLUSION

17. Overall, [*country name*] has made [*insert language giving an overall judgment about the totality of progress which has been made (e.g. Overall, the country has made good progress/some progress/minimal progress/no progress...)*] progress in addressing the technical compliance deficiencies identified in its MER and has been re-rated on [*insert the number of Recommendations which are re-rated*] Recommendations.

18. [Insert *a paragraph summarising which Recommendations are re-rated*]

19. [*Insert a paragraph summarising which Recommendations the country has made progress on, but for which a re-rating is not yet justified*]

20. [*Insert a paragraph summarising the progress on Recommendations which were amended after the MER was adopted (e.g. R.5 and R.8) and whether any re-ratings were given*]

21. Overall, in light of the progress made by [*country name*] since its MER was adopted, its *technical* compliance with the FATF Recommendations has been re-rated as follows [*Note: Proposed TC re-ratings should be in **bold italics** in the table below.*]

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

22. [*country name*] will [*remain in enhanced / remain in regular / move from enhanced to regular*] follow-up and will continue to report back to MONEYVAL on progress to strengthen its implementation of AML/CFT measures.

Appendix 7 – ANALYTICAL TOOL FOR TECHNICAL COMPLIANCE RE-RATINGS REQUESTS (NOT FOR PUBLICATION)

Instructions for assessed countries: Use the first 4 columns of this table to report back on what actions (if any) have been taken to address the technical deficiencies identified in your mutual evaluation report (MER), and implement new requirements where the FATF Standards have changed since your MER was adopted. As is the case with mutual evaluations, it is the responsibility of the assessed country to demonstrate that its AML/CFT system is compliant with the Recommendations. On this basis, the fourth column should explain the actions taken since the MER was adopted including cross-references to specific legislation, enforceable means, or other relevant mechanisms. All relevant legislation should be submitted with the below table.

Instructions for the [Secretariat and Rapporteur teams] responsible for analysing the actions taken by the assessed country: Analyse the information in the first 4 columns of the table, any additional supporting material provided by the assessed country, and the MER's analysis of other criteria (if any) that are not being reported on as no further action has been taken since the MER was adopted. On that basis, determine whether a re-rating is justified or not. Use the last column of this table to record your analysis and conclusions on the extent to which the actions taken by the assessed country to address the deficiency or meet the new requirements of the FATF Standards. After each Recommendation for which analysis is being undertaken, set out your conclusions concerning the rating (e.g. whether the rating should be upgraded, downgraded or remain the same).

Instructions for the Secretariat: This tool is an internal working document (not for publication) that should be circulated to delegations along with the standardised follow-up report (FUR) publication format (see the previous section), in advance of the working group/Plenary. The purpose of this tool is to present the detailed technical analysis systematically and in a structured way which streamlines delegations' prePlenary quality and consistency (Q&C) review and facilitates subsequent working group/Plenary discussions. Secretariats may wish to circulate this tool with a short introductory section setting out:

- the FATF/FSRB/Universal Procedures governing the process for FURs where TC re-ratings are requested, and
- the key decisions to be made based on the expectation that countries will have addressed most if not all technical compliance deficiencies by the end of the third year from the adoption of the MER (as per para.29 of the Universal Procedures). The key decisions may relate to requests for reratings, proposals to move countries from enhanced to regular follow-up, and/or proposals for the Plenary to consider applying other enhanced measures such as those listed in paragraph 80 of the FATF Procedures and paragraph 30 of the Universal Procedures.

Rec. No.	Criterion No.	Deficiency cited in MER/New requirements where FATF Standards have changed since MER *(Use 1 row per deficiency/new requirement)*	Actions taken (To be filled in by the country, along with the previous 3 columns)	Analysis & conclusions *(To be filled in by the Secretariat/group of experts/review group)*
[E.g.R.3]	[E.g. C.3.5]	[E.g. Quote the deficiencies for this criterion as reflected in the MER *Summary of Technical Compliance – Key Deficiencies* table]	[E.g. Briefly describe the actions taken to address the deficiencies for this criterion]	[E.g. Record your analysis and conclusions on the extent to which the actions taken by the assessed country address this deficiency]
[E.g.R.3]				[E.g. Recommendation XX is rated XX, based on progress made since the MER was adopted.]
[E.g.R.8]	[E.g. C.8.1]	[E.g. Where the FATF Standards have changed since the MER, quote the new requirements from the Methodology]	[E.g. Briefly describe the actions taken to address the new requirements for this criterion]	[E.g. Record your analysis and conclusions on the extent to which the actions taken by the assessed country meet the new requirements]
[E.g.R.8]				[E.g. The new requirements of Recommendation XX are rated XX, based on progress made since the MER was adopted.]

Appendix 8 – CONDUCTING MUTUAL EVALUATIONS DURING THE COVID-19 PANDEMIC

Overarching principles

1. Four overarching principles should guide MONEYVAL in its application of greater flexibility for using the so-called hybrid on-site visits (physical on-site visits with some virtual aspects), and its implementation of objective criteria and procedures for handling MEs during the COVID-19 crisis:

   a) As it is important for MONEYVAL to adapt and find ways to continue its assessment work during the COVID-19 crisis, in line with its mandates, on-site visits should proceed when it is possible to do so in a manner that respects these overarching principles. Postponements should occur only when absolutely necessary and should not be used as a means to delay implementation of the FATF Standards or gain unfair advantage in the assessment process. Decisions to postpone on-site visits should be based on objective criteria and procedures to avoid any arbitrariness.

   b) COVID-19 represents a serious global health risk. Consequently, the main priority for handling MEs during the pandemic is the health and safety of all participants. On-site visits should not jeopardise the health and safety of the national authorities, assessors or Secretariat staff. This takes precedence over any other consideration. Everything must be done to make the on-site visit as safe as possible.

   c) Greater flexibility granted to do some aspects of an on-site virtually, should be both in line with the intention set out in 1a. above of MONEYVAL adapting and continuing assessments and in line with keeping the quality of assessments and the integrity of the process. It is important to continue producing good quality mutual evaluation reports (MERs). The global network's commitment to quality and consistency (Q&C) at every stage of the ME process remains unchanged, as reflected throughout the *Universal Procedures*[218]. Consequently, an ME should not push ahead in circumstances likely to result in a poor quality report that has the potential to affect the credibility of the FATF brand. Hybrid on-site visits will not necessarily result in lower quality MERs, but MONEYVAL must take care and strive to achieve substantially the same level of quality with this new format. The following factors are considered essential to safeguard the quality of an assessment and the integrity of the process:

      (i) maintaining the physical nature of the on-site visit by requiring an adequate number of assessors with a broad range of expertise and supporting Secretariat staff to be physically present;

      (ii) requiring all assessors to participate effectively throughout the hybrid on-site visit without prejudice to the quality of the assessment, regardless of whether they are participating physically or virtually; and

      (iii) ensuring that the logistical and technical conditions of an on-site visit are sufficient to enable the assessed country to make its case fully, the assessors to do their work properly and have access to the authorities, and the Secretariat to support both parties adequately throughout the process.

   d) MONEYVAL will ensure that its approach is consistent with the global network, while at the same time in full respect of its own procedures and mandate.

Applying the principles-based approach to MONEYVAL evaluations

2. To enable the MONEYVAL to continue the ME process as required by its mandate, these procedures provide further flexibility on the composition of the onsite team, which is physically onsite. This is to allow for the virtual attendance of assessors and supporting

[218] See for examples paragraphs 11, 12, 25-26, 28, 31, 33 to 46 of the *Universal Procedures.*

Secretariat staff who are unable to attend in person because of the COVID-19 situation, provided the overarching principles above are respected.

Necessary conditions for a hybrid on-site visit

3. To safeguard the quality of assessments and integrity of the process (which is an overarching principle), such hybrid on-site visits may occur only if the following conditions are met:

   a) The physical nature of the on-site visit is maintained, albeit with flexibility to do some aspects virtually. This means that:

      (i) assessors who are experts in financial, legal, law enforcement and FIU issues must attend the on-site visit in person[219];

      (ii) at least two Secretariat staff should attend the on-site visit in person to support the assessed country and assessors[220] ; and

      (iii) all assessors and Secretariat staff who are unable to travel to the assessed country for reasons related to COVID-19 participate effectively in the on-site visit, as is envisaged by the *Universal Procedures* and *MONEYVAL Procedures for the 5th Round of Mutual Evaluations*.[221]

   b) The technical and logistical conditions of a hybrid on-site are sufficient to enable the assessed country to make its case fully, the assessors to do their work properly and have access to the authorities (including private sector, non-profit organisations where needed), and the Secretariat to support both parties adequately throughout the process. As is the current practice, whilst negotiating the on-site agenda, the host country should accommodate requests to visit agencies deemed important to achieving the purpose of the on-site visit (e.g., the FIU premises for IO.6). They should also be able to accommodate any other request for last-minute meetings, such as with private sector or civil society representatives (without presence of competent authorities).

      Overall, facilitating technical and logistical conditions of a hybrid on-site means all countries, delegations and the MONEYVAL Secretariat must do their best to facilitate the ME on-site process under these unusual circumstances, in line with the overarching principles. This may mean making additional arrangements to those planned for the onsite, such as replacing a videoconferencing service if the one used is not working and additional meetings organised to address any gaps caused by IT failures. The process will require patience, creativity and strong will by the parties to make this work.

      To the extent possible given budgetary restraints and availability of qualified assessors, this could include making efforts to seek participation of additional assessors to augment the assessment team and ensure the necessary physical presence of necessary expertise during the on-site.

Objective criteria

4. The following objective criteria respect the overarching principles and are relevant to determining if the conditions for a hybrid on-site are met (although not all will apply in every case):

[219] Ideally, this means having one assessor physically present for each of these areas, although the number may be less if any of those present have expertise in more than one of these areas.

[220] Both should be Secretariat staff who are responsible for working on the assessment (not just available substitutes) and one should be the Secretariat team lead. In joint FATF/MONEYVAL assessments, one should be from the FATF Secretariat and one should be from the MONEYVAL Secretariat (if the MONEYVAL Secretariat is fully participating in the process, which is not always the case due to resource constraints).

[221] In particular, see para.10 and 20 of the *Universal Procedures,* and para.19 and 34 of the *FATF Procedures.*

a) Is the assessed country able to host the on-site visit in a manner that respects the health and safety of all participants and preserves the physical nature of the on-site visit? Factors which may impact these criteria include:

   (i) domestic travel restrictions;

   (ii) country-wide lockdowns;

   (iii) restrictions on the number of people allowed to congregate;

   (iv) access to appropriate meeting venues;

   (v) sanitation precautions planned for the on-site visit;

   (vi) official assessments about the infection rate and spread of the COVID-19 virus; and

   (vii) other circumstances that create similar issues and are related to the COVID-19 pandemic.

b) Are enough assessors and Secretariat staff[222] (to preserve the physical nature of the on-site visit as described above in paragraph 3a) able to travel to the assessed country in a manner that respects their health and safety? Factors which may impact these criteria include:

   (i) travel restrictions prohibiting or strongly discouraging travel to the assessed country;[223]

   (ii) lengthy quarantine requirements (applying on arrival in the assessed country and/or on return to the traveller's home country) render travelling to the on-site and the related resource and cost commitment unreasonable;[224]

   (iii) the traveller's concerns about the availability and access to medical care should they fall ill during the on-site visit;

   (iv) a doctor has advised an individual against their travel to the assessed country for medical reasons; and

   (v) other circumstances that create similar issues and are related to the COVID-19 pandemic.

c) Are any assessors[225] (regardless of whether they are attending the on-site physically or virtually) unable to participate effectively in the process, as envisaged by the Universal and MONEYVAL Procedures? Factors which may impact these criteria include:

   (i) a country's ability or willingness to honour their commitment to provide an assessor;

   (ii) an assessor's inability or unwillingness to commit to working full time on the ME for the duration of the on-site visit, attend all meetings during the hybrid on-site visit, as normally they would be expected to attend and participate in a fully collaborative process as required by Rule 14 paragraph 14 of *MONEYVAL Procedures*; and

[222] This objective criteria should be mindful of the necessary conditions of a hybrid onsite, especially paragraph 3b. above, where all parties will do their best to facilitate the ME process mindful as well of any budgetary or other restraints.

[223] Travel restrictions may come from: 1) the assessed country; 2) the home country of the assessor or Secretariat staff; or 3) an international body such as the CoE, IMF and World Bank).

[224] Normally, a quarantine period of seven days or more would be considered overly lengthy, unless the country providing the assessor and the assessor are prepared to bear it. In cases where specific diplomatic measures can be made available by all the parties involved in the process in order to soften / exempt the quarantine requirements, the delays presented in this footnote may not be applicable. All parties are invited to do their best efforts to facilitate this process.

[225] This objective criteria should be mindful of the necessary conditions of a hybrid onsite, especially paragraph 3b. above, where all parties will do their best to facilitate the ME process mindful as well of any budgetary or other restraints.

(iii) other circumstances that create similar issues and are related to the COVID-19 pandemic.

d) Are the technical capabilities and logistical arrangements adequate to allow the assessed country to make its case fully, the assessors to do their work properly and have access to the authorities, and the Secretariat to support the process adequately? Factors which may impact these criteria include:

(i) access to adequate video conferencing facilities/platforms (e.g. Kudo, Bluejeans, Webex, Microsoft Teams, Zoom) for the assessed country and any assessors or Secretariat staff who are participating virtually;

(ii) the ability to have simultaneous interpretation for participants participating physically and virtually (where needed);

(iii) access to secure channels of communication for sharing confidential documents as needed;

(iv) measures[226] to ensure the confidentiality of information and discussions in the virtual environment, consistent with the existing procedures (para.19 UPs / Title VI of MONEYVAL procedures);

(v) allocating enough meeting time to allow for scheduling or technical difficulties associated with facilitating virtual participation, taking into account time zone differences and the organisation of the agenda as needed; and

(vi) other circumstances that create similar issues and are related to the COVID-19 pandemic.

Determining whether an on-site visit can take place

5. Subject to the overarching principles which take precedence in these matters:

a) where they are necessary, after exhaustion of all possibilities available using the overarching principles and objective criteria, postponements should be as brief as possible to minimise the impact on the assessment;

b) the criteria for postponing and resuming an assessment should be objective and apply equally to all countries impacted by the COVID-19 crisis; and

c) all decisions to postpone and resume on-site visits should respect the overarching principles, and the Plenary discussion of such reports should be rescheduled as soon as practicable. MONEYVAL recognises that postponements caused by the COVID-19 pandemic may delay completion of this round of mutual evaluations.

6. At least seven weeks prior to the on-site visit, the Secretariat, in consultation with the assessed country and assessors, will make initial inquiries, as to whether the on-site visit can take place in circumstances that respect the overarching principles in paragraph 1, and taking into account the necessary conditions for a hybrid on-site visit in paragraph 3 and the objective criteria noted above in paragraph 4.

7. The onus is on the affected party to provide the Secretariat with supporting information that shows their inability to host or travel to the on-site visit, while respecting the overarching principles.[227] In doing so, the affected party should give a full and detailed explanation in writing of how and to what extent the COVID-19 crisis (including crisis response measures)

[226] Such measures could include having all participants sign confidentiality agreements to govern their conduct during virtual meetings or implementing IT-based solutions.

[227] Assessed countries are encouraged to provide this information in the form of a letter to the Chair confirming their inability to host the on-site visit and citing the specific reasons why the on-site visit cannot be safely and in conditions that will safeguard the quality of the assessment. However, this is not a requirement as it may not be possible in all cases, including for reasons related to the COVID-19 crisis.

are negatively affecting their ability to proceed. Where relevant, this should include reference to the specific measures[228] or circumstances that are objectively preventing the on-site visit from moving forward consistent with the overarching principles.

8. If it appears from the material submitted that the on-site cannot take place, in line with the overarching principles, the Secretariat shall inform the Bureau and provide them with any relevant supporting documentation.

9. The Bureau will review the information submitted, taking into account the overarching principles in paragraph 1, the necessary conditions for a hybrid on-site visit in paragraph 3 and any relevant objective criteria in paragraph 4, to determine whether prima facie the on-site visit may proceed in line with the overarching principles. The Bureau will make the final determination, based on the overarching principles in paragraph 1, and taking into account the necessary conditions for a hybrid onsite visit in paragraph 3 and any relevant objective criteria in paragraph 4. In doing so, the Bureau will take into account the views of the assessed country, assessors and Secretariat.

10. Where the on-site visit is postponed, the delay may significantly impact the ability of the Plenary to discuss the report in a meaningful way. This is because the draft schedule of evaluations has been prepared to allow enough time between the on-site visit and the Plenary discussion. Where the onsite visit must be postponed, the Secretariat will write to the assessed country's head of delegation informing of the reasons why the on-site visit cannot proceed as scheduled and the need to defer discussion of the mutual evaluation report.

11. The postponement may result in the need to adjust the schedule of MONEYVAL Plenary meetings. If this is the case, the Secretariat in consultation with the Bureau shall determine new dates for the Plenary meeting(s) and provide an updated Workplan for information of MONEYVAL members.

12. If the Bureau determines that the on-site visit is able to proceed in line with the overarching principles, taking into account the necessary conditions for a hybrid on-site visit in paragraph 3 and any relevant objective criteria in paragraph 4, the Secretariat will write to the head of delegation confirming that the on-site visit will proceed as scheduled. The Secretariat will advise the assessors accordingly. In such cases, the assessed country, assessors and Secretariat should maintain an ongoing dialogue on the sanitary precautions and expectations that will be in place during the on-site visit to safeguard the health of all participants (e.g. regular cleaning of meeting rooms, expectations concerning the wearing of masks, arrangement to enable social distancing, etc.)

13. Ordinarily, this determination should be made six weeks before the on-site visit. However, because the COVID-19 situation is rapidly evolving, circumstances may change at any time leading up to (or during) the on-site visit and on very short notice. If any circumstances arise after the Secretariat has made its initial inquiries which could jeopardise the ability to hold the on-site in line with the overarching principles, the affected party should immediately inform the Secretariat and provide any relevant supporting information. In such cases, the procedures outlined in paragraphs 5 to 12 will be applied on an urgent basis.

Resuming the mutual evaluation

14. If the on-site visit has been postponed, the Secretariat shall continue consulting with the assessed country and assessors to find the earliest possible date to reschedule the on-site in circumstances where the overarching principles may be respected.

15. Leading up to the new dates of the on-site visit, the procedures outlined in paragraphs 5 to 12 shall be applied again (beginning at least seven weeks prior to the new date of the on-site visit) to determine whether or not the new on-site visit may take place or must be postponed further.

[228] For example, lockdowns, travel restrictions, transportation restrictions, etc.

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for *Combating the financing of terrorism*)
BNI	Bearer-Negotiable Instrument
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IN	Interpretive Note
ML	Money Laundering
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
R.	Recommendation
RBA	Risk-Based Approach
SR.	Special Recommendation
SRB	Self-Regulatory 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
UN	United Nations
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

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.
Asset recovery	The term asset recovery refers to the process of identifying, tracing, evaluating, freezing, seizing, confiscating and enforcing a resulting order for, managing, and disposing of (including returning or sharing), criminal property and property of corresponding value.
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 and bearer share warrants	*Bearer shares* refers to negotiable instruments that accord ownership in a legal person to the person who possesses the physical bearer share certificate, and any other similar instruments without traceability. It does not refer to dematerialised and/or registered forms of share certificate whose owner can be identified. *Bearer share warrants* refers to negotiable instruments that accord entitlement to ownership in a legal person who possesses the physical bearer share warrant certificate, and any other similar warrants or instruments without traceability. It does not refer to dematerialised and/or registered form of warrants or other instruments whose owner can be identified. It also does not refer any other instruments that only confers a right to subscribe for ownership in a legal person at specified conditions, but not ownership or entitlement to ownership, unless and until the instruments are exercised.

Terms	Definitions
Beneficial owner	In the context of legal persons, *beneficial owner* refers to the natural person(s) who ultimately[229] owns or controls a customer[230] and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person.[231] In the context of legal arrangements, beneficial owner includes: (i) the settlor(s); (ii) the trustee(s); (iii) the protector(s) (if any); (iv) each beneficiary, or where applicable, the class of beneficiaries and objects of a power; and (v) any other natural person(s) exercising ultimate effective control over the arrangement.[232] In the case of a legal arrangement similar to an express trust, beneficial owner refers to the natural person(s) holding an equivalent position to those referred above. When the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified.
Beneficiaries	Please refer to the IN to Recommendation 8.
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 or may become entitled to the benefit of any trust arrangement. A beneficiary can be a natural person or a legal person, or a legal 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 when they are set up but only a class of beneficiaries and 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, or following exercise of trustee discretion in the case of a discretionary trust. The accumulation period is normally co-extensive with the trust perpetuity period

[229] 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.

[230] This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

[231] The ultimate beneficial owner is always one or more natural persons. As set out in R.10, in the context of CDD it may not be possible to verify the identity of such persons through reasonable measures, and, to the extent that there is doubt about whether a person with a controlling ownership interest in a legal person is the ultimate beneficial owner, or where no natural person exerts control through ownership interests, the identity should be determined of the natural persons (if any) exercising control of the legal person through other means. Where no natural person is identified in that role, the natural person who holds the position of senior managing official should be identified and recorded as holding this position. This provision of R.10 does not amend or supersede the definition of who the *beneficial owner* is, but only sets out how CDD should be conducted in situations where the beneficial owner cannot be identified.

[232] Reference to "ultimate effective control" over trusts or similar legal arrangements includes situations in which ownership/control is exercised through a chain of ownership/control.

Terms	Definitions
	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[233] 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 a competent authorities.
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.

[233] This includes financial supervisors established as independent non-governmental authorities with statutory powers.

Terms	Definitions
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.
Criminal property	The term *Criminal property* refers to the following categories: a) proceeds of money laundering or predicate offences (including income or other benefits derived from such proceeds); b) instrumentalities used in or intended for use in, money laundering or predicate offences; c) property laundered; d) property that is used in, or intended or allocated for use in, the financing of terrorism, terrorist acts, or terrorist organisations; e) the proceeds of the financing of terrorism, terrorist acts, or terrorist organisations.
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.
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;

Terms	Definitions
	■ 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.
Designated non-financial businesses and professions	*Designated non-financial businesses and professions* means: a) Casinos[234] 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;

[234] References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

Terms	Definitions
	■ 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.
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.
Designation	The term *designation* refers to the identification of a person[235], 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

[235] Natural or legal.

Terms	Definitions
	▪ 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.
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, 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.[236] 2. Lending.[237] 3. Financial leasing.[238] 4. Money or value transfer services.[239] 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.);

[236] This also captures private banking.

[237] This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

[238] This does not extend to financial leasing arrangements in relation to consumer products.

[239] 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
	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. 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. [240] 13. Money and currency changing.
Foreign counterparts	Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the cooperation 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).
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	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

[240] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Terms	Definitions
domestic law	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.
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 and other similar legal arrangements. Examples of other similar arrangements[241] (for AML/CFT

[241] Similarity is assessed having regard to Article 2 of the Hague Convention on the law applicable to trusts and their recognition on the basis of whether legal arrangements have a similar structure or perform a similar function to an express trust.

Terms	Definitions
	purposes) may include but are not limited to fiducie, certain types of Treuhand, fideicomiso and Waqf.[242]
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.
Nominator	*Nominator* is an individual (or group of individuals) or legal person that issues instructions (directly or indirectly) to a nominee to act on their behalf in the capacity of a director or a shareholder, also sometimes referred to as a "shadow director" or "silent partner".
Nominee shareholder or director	*Nominee* is an individual or legal person instructed by another individual or legal person ("the nominator") to act on their behalf in a certain capacity regarding a legal person. *A Nominee Director* (also known as a "resident director") is an individual or legal entity that routinely exercises the functions of the director in the company on behalf of and subject to the direct or indirect instructions of the nominator. A Nominee Director is never the beneficial owner of a legal person. A *Nominee Shareholder* exercises the associated voting rights according to the instructions of the nominator and/or receives dividends on behalf of the nominator. A nominee shareholder is never the beneficial owner of a legal person based on the shares it holds as a nominee.

[242] Except in countries where Waqf are legal persons under Recommendation 24.

Terms	Definitions
Non-profit organisations	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.
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.
Supervisors	*Supervisors* refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("*financial supervisors*"[243]) 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

[243] Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

Terms	Definitions
	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.
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	Please refer to the IN to Recommendation 8.

Terms	Definitions
abuse	
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.
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*.[244] 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 non-professional (e.g. a person acting without reward on behalf of family).
Unique transaction reference number	Please refer to the IN. to Recommendation 16.
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;

[244] 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.

Terms	Definitions
	ii. exchange between one or more forms of virtual assets; iii. transfer[245] of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
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.

[245] 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.