DOCUMENT OF INTERNATIONAL MONETARY FUND AND FOR OFFICIAL USE ONLY

**IMMEDIATE ATTENTION**

SM/03/400

December 18, 2003

To: Members of the Executive Board

From: The Secretary

Subject: **Revised Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Standards—FATF Working Group Draft**

Attached for the **information** of the Executive Directors is a paper on the FATF working group's draft revised methodology for assessing compliance with anti-money laundering and combating the financing of terrorism (AML/CFT) standards. The staff would welcome comments from Fund members by **January 8, 2004**.

The staff intends to publish the methodology once it has been finalized.

The requested comments should be forwarded to Mr. Lalonde, Rlalonde@imf.org (MFD, ext. 38691) and Ms. SenGupta, psengupta@imf.org (LEG, ext. 30032), who are also available to answer questions on the paper.

This document will shortly be posted on the extranet, a secure website for Executive Directors and member country authorities.

Att: (1)

Other Distribution:
Department Heads

INTERNATIONAL MONETARY FUND

# Revised Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Standards: FATF Working Group Draft

Prepared by the
Monetary and Financial Systems and Legal Departments, IMF

Approved by Stefan Ingves and François Gianviti

December 17, 2003

1. Attached is a draft of the revised, comprehensive methodology for assessments of the standards for *anti-money laundering and combating the financing of terrorism (AML/CFT)*. The draft methodology is being circulated to Executive Directors for information and transmittal to members for their comment. The methodology is being prepared by a working group of the Financial Action Task Force (FATF), which includes Fund and Bank staff and representatives of the FATF-Style Regional Bodies (FSRBs), and other international organizations.

2. The AML/CFT methodology, which earlier was endorsed by the Executive Board for use in the AML/CFT assessments,[1] is being revised to reflect the significant changes made to the FATF 40 Recommendations for anti-money laundering that were adopted by the FATF in June 2003. Once the revised methodology is adopted by the FATF, the FSRBs, and the Fund and the Bank Boards, it would become the basis for future AML/CFT assessments world wide. Under existing Board guidance, the final text of the methodology to be presented to the Fund and Bank Boards will include italicized sections that identify those areas that are not assessed by the Fund and Bank staffs or experts under their supervision (i.e., the assessment of law-enforcement measures and the implementation of preventive measures for non-prudentially regulated financial sectors that are not macroeconomically relevant, but are nonetheless vulnerable to money laundering).

3. On December 10, 2003, the FATF working group forwarded the attached draft methodology to the Fund, the World Bank, and standard setters, requesting comments by January 10, 2004. **In view of the working group's short time line, the staff would welcome comments from Fund members by January 8, 2004,** which staff would then forward to the FATF working group for consideration. After all comments have been considered, a final draft of the methodology will be presented for endorsement by the FATF Plenary, February 25–27, 2004, and subsequently for consideration for endorsement by the Fund and Bank Boards as part of the review of the AML/CFT pilot program, which is scheduled for discussion in March 2004.

---

[1] SM/02/349, November 8, 2002.

4. The staff wishes further to inform Executive Directors that many Fund members have already had an opportunity to comment on an earlier version of the draft methodology by virtue of their membership in the FATF or an FSRB. To avoid duplication in the submissions of comments, the staff would be pleased to receive only those additional comments that were not also provided through the FATF or an FSRB.

# METHODOLOGY FOR ASSESSING COMPLIANCE WITH ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM STANDARDS 2003

## Introduction

*[DG to review status of additional criteria, the differing requirements in the FATF 40 + 8 Recommendations such as "should", "should be required", "should consider", "are encouraged" etc. Also to consider particularly §5, 10 & 11, 13, key definitions in §16, 17 & 18 (content and formatting), definition of "law or regulation and other enforceable means", implementation issue in §25, etc],*

This document consists of three sections. Following this introduction, the first section consists of an overview of the assessment methodology, its background, a description of the structure of the document, and of certain conditions that are not included in the assessment criteria but that are nevertheless necessary for an effective anti-money laundering and combating the financing of terrorism ("AML/CFT") system. The second section consists of guidance and interpretation concerning the Methodology, the criteria and compliance, and the terminology that is used. Finally, the third section sets out the AML/CFT assessment criteria themselves.

## The AML/CFT Assessment Methodology

### Background to Methodology

1. The Anti-Money Laundering/Combating Terrorist Financing (AML/CFT) Methodology 2003, including the assessment criteria, is designed to guide the assessment of a country's[1] compliance with the international AML/CFT standards as contained in the FATF Forty Recommendations 2003 and the FATF Eight Special Recommendations on Terrorist Financing 2001 (referred to jointly as the FATF Recommendations). The Methodology is a key tool to assist assessors when they are preparing AML/CFT detailed assessment reports/mutual evaluation reports.

2. It is based on the AML/CFT Methodology issued in October 2002, but is revised to take into account the significant revisions that were made in the Forty Recommendations 2003. It is also informed by the assessment experience of the FATF and the FATF-style regional bodies (FSRBs) (from their mutual evaluations), of the International Monetary Fund (the Fund) and the World Bank (the Bank)(in the Financial Sector Assessment Program (FSAP)) and by the Fund (in the Offshore Financial Center assessment program (OFC)). The FATF, the Fund and the Bank have also reviewed the assessments/mutual evaluations conducted in 2002 and 2003 using the AML/CFT Methodology issued in October 2002, and these reviews have also provided guidance in developing this Methodology.

3. [The Methodology was agreed by the FATF Plenary at its meeting in February 2004, and approved by the Executive Boards of the Fund and the Bank in March 2004. [The following FSRBs have also endorsed the Methodology: .]]

### The Structure of the Methodology Document

4. An effective AML/CFT system requires an adequate legal and institutional framework, which should include: (i) laws that create money laundering (ML) and terrorist financing (FT) offences and provide for the freezing, seizing and confiscation of the proceeds of crime and terrorist funding; (ii) laws, regulations or in certain circumstances other enforceable means that impose the required obligations on financial institutions and designated non-financial businesses and professions; (iii) an appropriate institutional or administrative framework, and laws that provide competent authorities with the necessary

[1] All references to "country" in this Methodology include territories or jurisdictions. See paragraph 16.

duties, powers and sanctions; and (iv) laws and other measures that give a country the ability to provide the widest range of international co-operation . It is also essential that the competent authorities ensure that the whole system is effectively implemented.

5. It should be noted that in some countries, 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. For example, profit generating criminal offences may exist at both federal and state levels, and thus measures to combat money laundering should be taken at the state/provincial level. When evaluations or assessments are being conducted, appropriate steps should be taken to ensure that AML/CFT measures at the state/provincial level are also adequately addressed.

6. The Methodology follows the structure of the FATF Recommendations. However, as the Methodology is a tool to assist assessors in determining whether countries are in compliance with the FATF Recommendations, it is not intended that detailed assessment reports/mutual evaluation reports will rigidly follow the format and structure of the Methodology. Rather the format for these reports will be based on the four fundamental areas noted in paragraph 4 above. The assessments will also need to be based on and refer to relevant underlying information, such as the quantum and type of predicate offences for money laundering; the vulnerability of the country to money laundering or terrorist financing, the methods, techniques and trends used to launder money or fund terrorists; the structure of the financial system and the nature of the sectors dealing with designated non-financial businesses and professions; the nature of the underlying criminal justice system, as well as any changes that have been made to the AML/CFT system in the relevant period. Most importantly, the format of the reports will allow for an assessment of whether the Recommendations have been fully and properly implemented and the AML/CFT system is effective. As in previous FATF evaluation rounds, this could be judged by reference to quantitative data and the results that have been achieved, or could be based upon more qualitative factors.

### Other factors necessary for an effective AML/CFT system

7. An effective AML/CFT system requires that certain structural elements, not covered by the AML/CFT assessment criteria, also be in place. The lack of such elements, or significant weaknesses or shortcomings in the general framework, may significantly impair the implementation of an effective AML/CFT framework. Although the AML/CFT assessment criteria do not cover these conditions, apparent major weaknesses or shortcomings identified should be noted in the mutual evaluation/detailed assessment report. These elements should include in particular:

a) sound and sustainable macro-economic policies;
b) a well-developed public sector infrastructure, having regard to the level of economic development of the country;
c) the respect of principles such as transparency and good governance;
d) a proper culture of AML/CFT deterrence shared and reinforced by government, financial institutions, designated non-financial businesses and professions; industry trade groups, and self-regulatory organisations (SROs);
e) appropriate measures to combat corruption;
f) a reasonably efficient court system that ensures that judicial decisions are properly enforced;
g) high ethical and professional requirements for police officers, prosecutors, judges, etc. and measures and mechanisms to ensure these are observed;
h) a system for ensuring the ethical and professional behaviour on the part of professionals such as accountants and auditors, and lawyers. This may include the existence of codes of conduct and good practices, as well as methods to ensure compliance such as registration, licensing, and supervision or oversight.

## Guidance on the Criteria, the Compliance ratings, and General Interpretation concerning the AML/CFT Standards and Methodology

### The Criteria and Compliance

8. The assessment of the adequacy of a country's AML/CFT framework will not be an exact process, and the vulnerabilities and risks that each country has in relation to ML and FT will be different depending on domestic and international circumstances. ML and FT techniques evolve over time, and therefore AML/CFT policies and best practices will also need to develop and adapt to counter the new threats.

9. The FATF Recommendations provide the international standard for combating money laundering and terrorist financing and the Recommendations and the criteria set out in this Methodology 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, it is acceptable that countries implement the international standards in a manner consistent with their national legislative and institutional systems, even though the methods by which compliance is achieved may differ. In this regard, assessors should be aware of each country's stage of economic development, its range of administrative capacities, and different cultural and legal conditions. Moreover, the report should provide the context for the assessment, and make note of any progress that has been or is being made in implementing the international standards and the criteria in this Methodology.

#### The Criteria

10. The following set of criteria for each of the FATF Recommendations are listed under two separate headings: "essential criteria" and "additional criteria". The essential criteria are those elements that should be present in order to demonstrate full compliance with a Recommendation. The additional criteria are optional elements that further strengthen the AML/CFT system and may be desirable.

11. The essential criteria are based on the FATF Recommendations, though in a limited number of criteria the wording of the criteria may go beyond the literal wording of the Recommendations e.g. criteria 1.2. The additional criteria are derived from non-mandatory requirements in the FATF Recommendations or on Best Practice and other guidance issued by the FATF, or by the Basel Committee on Banking Supervision. As the essential criteria are the elements that must all be met to comply with the FATF Recommendations, they also provide the basis for any self-assessment exercises.

12. Criteria to be assessed are numbered sequentially for each Recommendation, but the sequence of criteria is not important [– all essential criteria are equally important in determining whether a country is compliant with a Recommendation]. In some cases elaboration (indented below the criteria) is provided in order to assist in identifying important aspects of the assessment of the criteria.

#### Compliance Ratings

13 For each Recommendation there are four possible levels of compliance: compliant, largely compliant, partially compliant, and non-compliant. A country is compliant with a Recommendation whenever the Recommendation is fully observed. A requirement is considered largely compliant when there are only minor shortcomings or a large majority of the essential criteria are fully met, and there are no major concerns. A requirement is considered partially compliant when the country has taken some action and complies with some of the essential criteria, but several essential criteria or key essential criteria are not met. A requirement is considered non-compliant whenever the country has not addressed the issue or has addressed it in a manner that cannot reasonably lead to compliance with any of the essential criteria. A requirement or part of a requirement is considered not applicable whenever, in the view of the assessor, the requirement does not apply, given the structural, legal and institutional features of a country e.g. a particular type of financial institution does not exist in that country.

14. Assessors should review whether the laws and regulations meet the appropriate standard and whether there is adequate capacity and implementation of those laws. Countries should only be regarded as fully complying with criteria if the relevant laws, regulations or other AML/CFT measures are in force and effect at the time of the on-site visit to the country or in the period immediately following the on-site mission, and before the finalisation of the report.

15. Laws 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 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 this Methodology. Assessors should be aware of, and have regard to any assessments or findings made with respect the Core Principles. 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.

## General Interpretation and Guidance

16. Set out below are key definitions from the FATF Recommendations that are used throughout the Methodology[2], and guidance on other points of general interpretation.

**Countries** – all references in the FATF Recommendations and in this Methodology to "countries" apply equally to "territories" or "jurisdictions".

**Designated non-financial businesses and professions (DNFBP)** means:

a) Casinos (which also includes internet casinos).
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 measures that would combat money laundering.
f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust[3];
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

---

[2] A full set of definitions from the Forty Recommendations and the Eight Special Recommendations are at Annexes 2 & 3.

[3] 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 e.g. constructive trust.

**Financial Institutions**[4] means:

"Any person or entity 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.[i]
2. Lending.[ii]
3. Financial leasing.[iii]
4. The transfer of money or value.[iv]
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, CDs, derivatives etc.);
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
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.[v]
13. Money and currency changing.

i. This also captures private banking.
ii. This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).
iii. This does not extend to financial leasing arrangements in relation to consumer products.
iv. This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. 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 Interpretative Note to Special Recommendation VII.
v. This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

**Financing of terrorism** (FT) includes the financing of terrorist acts, and of terrorists and terrorist organisations.

**Should** – For the purposes of assessing compliance with the FATF Recommendations, the word "should" has the same meaning as "must".

**Supervisors** refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

---

[4] As an aide-memoire for assessors, Annex 1 to the Methodology sets out a list of examples of types of financial institutions that engage in the financial activities referred to in the definition.

17. **Requirements for financial institutions and designated non-financial businesses and professions** - The FATF Recommendations state that financial institutions or designated non-financial businesses and professions "should" or "should be required by law or regulation to" take certain actions. These references require countries or their competent authorities to take measures that will oblige their financial institutions or designated non-financial businesses and professions to comply with each of the relevant Recommendations. In the Methodology, in order to use one consistent phrase, the criteria relevant to financial institutions use the phrase "Financial institutions should be required" (a similar approach is taken for designated non-financial businesses). The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation[5] and the criteria that are basic obligations are marked with an asterisk (*). More detailed elements in Recommendations 5, 10 and 13, as well as obligations under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority[6].

18. **Consider** - references in the Recommendations that require a country to "consider" taking particular measures means that the country should have made a proper consideration or assessment of whether to implement such measures, including reaching justified conclusions. Evidence of that assessment should be available to assessors.

19. **Assessment for designated non-financial businesses and professions** - Under Recommendations 12 and 16 designated non-financial businesses and professions should be required to take certain actions. Assessors should assess compliance on the basis that all the designated categories of non-financial businesses and professions should meet the requirements set out in the Recommendation. However, it is not necessary to require these actions through laws, regulations or other 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, regulations or other enforceable means covering the underlying activities. Assessors should note that compliance by designated non-financial businesses and professions with all the necessary AML/CFT measures is to be assessed under Recommendations 12 & 16, and not under other Recommendations.

20. **Risk of money laundering or terrorist financing** - For each Recommendation and each criteria where a financial institution should be required to take certain actions, assessors should normally assess compliance on the basis that all financial institutions should have to meet all the specified requirements. However, a relevant consideration underlying the FATF Recommendations is the degree of risk of money laundering or terrorist financing for particular types of financial institutions or for particular types of customers, products or transactions. A country may therefore take risk[7] into account, and in the circumstances set out below, and subject to the relevant conditions being met, it may decide to limit the application of certain FATF Recommendations (either fully or in part).

21. The circumstances and conditions are:

(a) When a financial activity referred to in the definition of "financial institution" above is carried out on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering or terrorist financing activity occurring. An example might be a hotel providing money exchange facilities to guests, where the limit on the amount that can be exchanged is small.

(b) In other circumstances where there is a proven low risk of money laundering and terrorist financing, a country may decide not to apply some or all of the requirements in one or more Recommendations. However, this should only be done on a strictly limited and justified basis.

---

[5] **Law or regulation** refers to primary and secondary legislation, such as laws, decrees, regulations, or other similar requirements, usually issued under the authority of a legislative body, and which impose mandatory requirements.

[6] **Other enforceable means** refers to guidelines or other documents or mechanisms (other than laws or regulations) that set out enforceable requirements for which there are sanctions for non-compliance (see R.17), and which are issued by a competent authority or appropriately authorised person or body.

[7] All references to "risk" in this Methodology refer to the risk of money laundering and/or terrorist financing.

For the purposes of this Methodology, assessors should be satisfied as to the adequacy of the process to determine low risk and the reasonableness of the conclusions.

22. In Recommendation 5 there are a number of criteria which allow countries to permit their financial institutions to take risk into account when determining the extent of the customer due diligence measures that the institution must take. This should not allow financial institutions to completely avoid doing the required measures, but could allow them to reduce or simplify the measures they have to take for certain criteria. Assessors need to be satisfied that there is an adequate mechanism by which competent authorities assess or review the procedures adopted by financial institutions to determine the degree of risk and how they manage that risk, as well as to review the determinations made by institutions.

23. In Recommendations 5 and 9, reference is made to a financial institution being satisfied as to a matter. This also requires that the institution must be able to justify its assessment to competent authorities, and that assessors need to be satisfied that there is an adequate mechanism by which competent authorities can review the assessments of financial institutions.

24. **Use of examples** – in a number of Recommendations, for particular criteria, examples are provided of situations in which a particular requirement should apply, or where there may be exceptions to the normally applicable obligations. The examples are not part of the criteria, and are only illustrative. However, assessors should use them as guidance as to whether national measures for particular criteria may be appropriate.

25. **Effective implementation** – it is essential that all the FATF Recommendations are effectively implemented, and that assessments or evaluations address this. For some Recommendations this may only require, for example, that the necessary law or regulation has been enacted and is in force, while for others it may require both the law as well as other implementing measures. In certain Recommendations specific types of implementation measures or processes that must be taken are mentioned.

# THE FORTY RECOMMENDATIONS - CRITERIA

## A. LEGAL SYSTEMS

*Scope of the Criminal Offence of Money Laundering*

**Recommendation 1**

The criteria listed below should be read in conjunction with the text of Recommendation 1, Special Recommendation II, and the definition of "designated categories of offences" in the Glossary. (Note to assessors: Ensure that the assessments of Criteria 1.3 – 1.6 and Criteria II.2 – II.3 (in SR.II) are consistent.)

**Essential criteria**

1.1 Money laundering should be criminalised on the basis of the 1988 UN Convention Against Illicit Traffic in Narcotic Drugs and Pyschotropic Substances (the Vienna Convention) and the 2000 UN Convention Against Transnational Organized Crime (the Palermo Convention) i.e. the physical and material elements of the offence (see Article 3(1)(b)&(c) Vienna Convention and Article 6(1) Palermo Convention).

1.2 The offence of ML 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.

1.3 The predicate offences for money laundering should cover all serious offences, and countries should seek to extend this to 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. Where the designated category is limited to a specific offence, then that offence must be covered.

1.4 Where countries apply a threshold approach or a combined approach that includes a threshold approach[8], predicate offences should at a minimum comprise all offences:

a) that fall within the category of serious offences under their national law; or
b) which are punishable by a maximum penalty of more than one year's imprisonment; or
c) which 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).

Examples of categories of serious offences include: "indictable offences" (as opposed to summary offences), "felonies" (as opposed to misdemeanours); "crimes" (as opposed to délits).

1.5 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.

1.6 The offence of money laundering should apply to persons who commit the predicate offence. However, 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.

[8] Countries determine the underlying predicate offences for money laundering 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.

1.7 There should be appropriate ancillary offences to the offence of money laundering[9], including conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

**Additional criteria**

1.8 Countries may provide that it is a money laundering offence in circumstances where the proceeds of crime are derived from conduct that occurred in another country, which is not an offence in that other country but which would have constituted a predicate offence had it occurred domestically.

[9] Subsequent references in this Methodology to a money laundering (ML) offence refer not only to the primary offence or offences, but also to ancillary offences.

## Recommendation 2

The criteria listed below should be read in conjunction with the text of Recommendation 2.

### Essential criteria

2.1 The offence of ML should apply at least to natural persons that knowingly engage in ML activity.

2.2 The law should permit the intentional element of the offence of ML to be inferred from objective factual circumstances.

2.3 The offence of ML should extend to legal persons (e.g., companies, foundations), and, where that is not possible, civil or administrative liability should apply.

*[DG to add examples of "where that is not possible"]*

2.4 Making legal persons subject to criminal liability for ML should not preclude the possibility of parallel criminal, civil or administrative proceedings in countries in which more than one form of liability is available.

2.5 Natural and legal persons should be subject to effective, proportionate and dissuasive criminal, civil or administrative sanctions for ML.

*Provisional Measures and Confiscation*

## Recommendation 3

The criteria listed below should be read in conjunction with the text of Recommendation 3 and Special Recommendation III. (Note to assessors: Ensure that the assessments of Criteria 3.1 – 3.4, Criterion 3.6 and Criterion III.11 (in SR.III) are consistent.)

### Essential criteria

3.1 Laws should provide for the confiscation of property[10] that has been or is:

a) laundered;
b) proceeds from;
c) instrumentalities used in; and
d) instrumentalities intended for use in

the commission of any ML, FT or other predicate offences, and property of corresponding value (referred to as "property subject to confiscation").

3.1.1 Criteria 3.1 should equally apply to property that is derived directly or indirectly from proceeds of crime; including income, profits or other benefits from the proceeds of crime.

3.2 Laws and other measures should provide for provisional measures, including the freezing and/or seizing of property, to prevent any dealing, transfer or disposal of property that is or may become subject to confiscation.

3.3 Laws or 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.

3.4 Law enforcement agencies, the FIU or other competent authorities should be given adequate powers to identify and trace property that is, or may become subject to confiscation or is suspected of being the proceeds of crime.

3.5 Laws and other measures should provide protection for the rights of bona fide third parties. Such protection should be consistent with the standards provided in the Palermo Convention.
*[DG to review]*

3.6 There should be authority to take steps to prevent or void actions, whether contractual or otherwise, where the persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in their ability to recover property subject to confiscation.

### Additional criteria

3.7 Countries may consider laws that provide for the confiscation of:

a) The property of organisations that are found to be primarily criminal in nature (i.e. organisations whose principal function is to perform or assist in the performance of illegal activities).

---

[10] 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.

b) Property subject to confiscation, but without a conviction of any person (*civil forfeiture*), in addition to the system of confiscation triggered by a criminal conviction.

c) Property subject to confiscation, and which require an offender to demonstrate the lawful origin of the property

## B. MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NON-FINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

### Recommendation 4

The criteria listed below should be read in conjunction with the text of Recommendation 4.

### Essential criteria

4.1 Countries should ensure that no financial institution secrecy law will inhibit the implementation of the FATF Recommendations. 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 R.7, R.9 or SR.VII.

***Customer Due Diligence and Record-keeping***

## Recommendation 5

The criteria listed below should be read in conjunction with the text of Recommendations 5 and 8, Special Recommendation VII, the Interpretative Notes to Recommendation 5, 12 and 16, and to Recommendation 5, and the definitions of "beneficial owner", "designated threshold", "legal arrangements" and "legal persons" in the Glossary. (Note to assessors: Ensure that the assessments of Criteria 5.2 – 5.3 and Criterion VII.1 (in SR.VII) are consistent.)

### Essential criteria

5.1* Financial institutions should not be permitted to keep anonymous accounts[11] or accounts in fictitious names.

*Note to assessors [add reference to wire transfers]*

Where numbered accounts exist, financial institutions should be required to maintain them in such a way that full compliance can be achieved with the FATF Recommendations. For example, the financial institution should properly identify the customer in accordance with these criteria, and the customer identification records should be available to the AML/CFT compliance officer, other appropriate staff and competent authorities.

*When CDD is required*[12]

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

a) establishing business relations;
b) carrying out occasional transactions above the applicable designated threshold (USD/€ 15,000). This also includes situations where the transaction is carried out in a single operation or in several operations [if factual indications exist that there is a connection between those operations] [that appear to be linked];
c) carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII;
d) there is a suspicion of money laundering or terrorist financing, 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*[13]

5.3* Financial institutions should be required to identify the customer (whether permanent or occasional) and verify that customer's identity using reliable, independent source documents, data or information[14].

---

[11] The reference to "accounts" should be read as including other similar business relationships between financial institutions and their customers.

[12] Financial institutions do not have to repeatedly perform identification and verification every time that a customer conducts a transaction.

[13] The general rule is that customers should be subject to the full range of CDD measures. However, there are circumstances in which it would be reasonable for a country to allow its financial institutions to apply the extent of the CDD measures on a risk sensitive basis.

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

5.3.1[*] For customers that are natural persons, the financial institution should be required to obtain sufficient identification data to be satisfied[15] as to the identity of the customer[16].

5.3.2[*] For customers that are legal persons or legal arrangements, the financial institution should be required to:

(a) verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person; and
(b) verify the legal status of the legal person or legal arrangement, e.g. by obtaining proof of incorporation or similar evidence, and obtain information concerning the customer's name, the names of trustees, *[DG to review]* legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement.

5.4* Financial institutions should be required to identify the beneficial owner[17], and take 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.

5.4.1* For all customers, the financial institution should determine whether the customer is acting on behalf of another person, and should then take reasonable steps to obtain sufficient identification data to verify the identity of that other person[18].

5.4.2[*] For customers that are legal persons or legal arrangements, the financial institution should be required to:

(a) take reasonable measures to understand the ownership and control structure of the customer;
(b) determine who are the natural persons that ultimately own or control the customer. This includes those persons who exercise ultimate effective control over a legal person or arrangement.

Examples of the types of measures that would be normally needed to satisfactorily perform this function include:

- For companies - identifying the natural persons with a controlling interest and the natural persons who comprise the mind and management of company.
- For trusts - identifying the settlor, the trustee or person exercising effective control over the trust, and the beneficiaries.

Relevant information or data should be obtained from a reliable source, which could be a public register, the customer or other reliable sources.

Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements i.e. a public company listed on a recognised stock exchange, it is not necessary to seek to identify and verify the identity of the [controlling] shareholders of that company as such information should be publicly available.

---

[15] 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.

[16] Examples of the types of customer information that could be obtained, and the identification data that could be used to verify that information is set out in the paper entitled General Guide to Account Opening and Customer Identification issued by the Basel Committee's Working Group on Cross Border Banking.

[17] "Beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

[18] Financial institutions engaged in insurance business, as set out under item 12 in the definition, must identify and verify the identity of the policy holder (the customer) and the beneficiary under the insurance contract (where that person is different to the policy holder).

5.5 Financial institutions should be required to obtain information on the purpose and intended nature of the business relationship.

5.6* Financial institutions should be required to conduct ongoing due diligence on the business relationship.

5.6.1 Ongoing due diligence should include 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, and where necessary, the source of funds.

5.6.2 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 regular reviews of existing records, particularly for higher risk categories of customers or business relationships.

5.7 Where financial institutions are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by the competent authorities.

*Risk*

5.8 Financial institutions should be required to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction.

Examples of higher risk categories (which are derived from the Basle CDD Paper) may include

a) Non-resident customers,
b) Private banking,
c) Legal persons or arrangements[such as trusts,] that are personal assets holding vehicles,
d) Companies that have nominee shareholders or shares in bearer form.

Types of enhanced due diligence measures may include those set out in Recommendation 6.

5.9 Countries may permit financial institutions to take reduced or simplified CDD measures only when the risk of money laundering or terrorist financing has been determined to be lower. The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

Examples of customers, transactions or products where the risk may be lower[19] could include:

a) Financial institutions – provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those requirements.
b) Public companies that are subject to regulatory disclosure requirements. This refers to companies that are listed on a stock exchange or similar situations.
c) Government administrations or enterprises.
d) Life insurance policies where the annual premium is no more than USD/€1000 or a single premium of no more than USD/€2500.

[19] Assessors should determine in each case whether the risks are lower having regard to the type of customer, product or transaction, or the location of the customer.

e) Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.

f) 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.

g) Beneficial owners of pooled accounts held by DNFBP provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring compliance with those requirements.

5.10 Where financial institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, the competent authority should limit this to countries that it has determined are in compliance with and have effectively implemented the FATF Recommendations. *[DG to review with respect to IN.13]*

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

*Timing of verification*

5.12 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.

5.13 Countries may permit financial institutions to complete the verification of the identity of the customer and beneficial owner following 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.

Examples of situations where it may be permitted are:

- 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.
- Life insurance business – in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

(c) The money laundering risks are effectively managed.

Where a customer is permitted to utilise the business relationship prior to verification, financial institutions should be required to adopt risk management procedures concerning the conditions under which this may occur. 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 of expected norms for that type of relationship.

*Failure to satisfactorily complete CDD*

5.14 Where the financial institution is unable to comply with Criteria 5.3. to 5.5. above, it should:

a) not be permitted to open the account, to commence business relations and to perform the transaction; and
b) consider making a suspicious transaction report.

5.15 Where the financial institution has already commenced the business relationship e.g. when Criteria 5.2(e), 5.13 or 5.16 apply, and the financial institution is unable to comply with Criteria 5.3 to 5.5 above it should be required to terminate the business relationship.

*Existing customers*

5.16 Financial institutions should be required to apply CDD requirements to existing customers[20] on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times.

For financial institutions engaged in banking business (and for other financial institutions where relevant) - examples of when it may otherwise be an appropriate time to do so is when: (a) a transaction of significance takes place, (b) customer documentation standards change substantially, (c) there is a material change in the way that the account is operated, (d) the institution becomes aware that it lacks sufficient information about an existing customer.

5.17 Financial institutions should be required to perform CDD measures on existing customers if they are customers to whom Criteria 5.1 applies.

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

## Recommendation 6

The criteria listed below should be read in conjunction with the text of Recommendation 6, its Interpretative Note, and the definition of "politically exposed persons" (PEPS) in the Glossary.

### Essential criteria

6.1 Financial institutions should be required, in addition to performing the CDD measures required under R.5, to put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person.

> Examples of measures that could form part of such a risk management system include seeking relevant information from the customer, referring to publicly available information or having access to commercial electronic databases of PEPS.

6.2 Financial institutions should be required to obtain senior management approval for establishing business relationships with a PEP.

6.2.1 Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, financial institutions should be required to obtain senior management approval to continue the business relationship.

6.3. Financial institutions should be required to take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPS.

6.4. Where financial institutions are in a business relationship with a PEP, they should be required to conduct enhanced ongoing monitoring on that relationship.

### Additional criteria

6.5 Countries should consider extending the requirements of R.6 to PEPS who hold prominent public functions in their own country. (Note: the Interpretative Note encourages countries to do this)

## Recommendation 7

The criteria listed below should be read in conjunction with the text of Recommendation 7 and the definition of "payable-through accounts" in the Glossary.

### Essential criteria

In relation to cross-border correspondent banking[21] and other similar relationships[22] financial institutions should, in addition to performing any CDD measures that may be required under R.5, be required to take the measures set out in Criteria 7.1-7.5.

7.1 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.

7.2 Assess the respondent institution's AML/CFT controls, and ascertain that they are adequate and effective.

7.3 Obtain approval from senior management before establishing new correspondent relationships.

7.4 Document[23] the respective AML/CFT responsibilities of each institution.

7.5 Where a correspondent relationship involves the maintenance of "payable-through accounts", financial institutions should be satisfied that:

(a) their customer (the respondent financial institution) has performed all the normal CDD obligations set out in R.5 on those of its customers that have direct access to the accounts of the correspondent financial institution; and
(b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

---

[21] 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 of funds, cheque clearing, payable-through accounts and foreign exchange services.

[22] [Similar relationships to which financial institutions should apply Criteria 7.1-7.5 include those established for securities transactions, funds transfers, or other financial transactions, whether for the cross-border financial institution as principal or for its customers].

[23] [It is not necessary that the two financial institutions always have to reduce the respective responsibilities into a written form provided there is a clear understanding as to which institution will perform the required measures]

## Recommendation 8

The criteria listed below should be read in conjunction with the text of Recommendation 8.

### Essential criteria

8.1 Financial institutions should be required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.

8.2 Financial institutions should be required to have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. These policies and procedures should apply when establishing customer relationships and when conducting ongoing due diligence.

Examples of non-face to face operations include: business relationships concluded over the Internet or by other means such as through the post, services and transactions over the Internet including trading in securities by retail investors over the Internet or other interactive computer services, use of ATM machines, telephone banking, transmission of instructions or applications via facsimile or similar means and making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or reloadable or account-linked value cards.

8.2.1 Measures for managing the risks should include specific and effective CDD procedures that apply to non-face to face customers.

Examples of such procedures include: the certification of documents presented; the requisition of additional documents to complement those which are required for face-to-face customers; develop independent contact with the customer; rely on third party introduction (see criteria 9.1 to 9.5) and require the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

Financial institutions should refer to the CDD Paper, Section 2.2.6.

For electronic services, financial institutions could refer to the "Risk Management Principles for Electronic Banking" issued by the Basel Committee in July 2003.

## Recommendation 9

The criteria listed below should be read in conjunction with the text of Recommendation 9 and its Interpretative Note.

Note: This Recommendation does not apply to:

(a) outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the financial institution to carry out its CDD functions[24];
(b) business relationships, accounts or transactions between financial institutions for their clients which are addressed by R.5 and R.7. *[DG to review reference to R.5]*

## Essential criteria

If financial institutions are permitted to rely on intermediaries or other third parties[25] to perform some of the elements of the CDD process (Criteria 5.3 to 5.5)[26] or to introduce business, then the following criteria should be met.

9.1 Financial institutions relying upon a third party should be required to immediately obtain from the third party the necessary information[27] concerning certain elements of the CDD process (Criteria 5.3 to 5.5).

9.2 Financial institutions should be required to take adequate steps to satisfy themselves 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.

9.3 Financial institutions should be required to satisfy themselves that the third party is regulated and supervised [or monitored] for (in accordance with Recommendations 23 or 24), and has measures in place to comply with, the CDD requirements set out in R.5 and R.10.

9.4 In determining in which countries the third party that meets the conditions can be based, competent authorities should take into account information available on whether those countries adequately apply the FATF Recommendations[28].

9.5 The ultimate responsibility for customer identification and verification should remain with the financial institution relying on the third party.

---

[24] Where there is a contract to outsource CDD, R.9 does not apply because the outsource or agent is to be regarded as synonymous with the financial institution i.e. the processes and documentation are those of the financial institution itself

[25] Intermediaries or other third parties can be financial institutions, DNFBP or other reliable persons or businesses that meet Criteria 9.1 to 9.4.

[26] In practice, this reliance on third parties often occurs through introductions made by another member of the same financial services group, or in some jurisdictions from another financial institution or third party. It may also occur in business relationships between insurance companies and insurance brokers/agents, or between mortgage providers and brokers.

[27] It is not necessary to obtain copies of documentation.

[28] Countries should refer to reports, assessments or reviews concerning AML/CFT that are published by the FATF, FSRBs, the IMF or World Bank.

**Recommendation 10**

The criteria listed below should be read in conjunction with the text of Recommendation 10 and its Interpretative Note.

**Essential criteria**

10.1* Financial institutions should be required to maintain all necessary records on transactions[29], both domestic and international, for at least five years following completion of the transaction (or longer if requested by a competent authority in specific cases and upon proper authority). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated.

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

Examples of the necessary components of transaction records include: customer's (and beneficiary's) name, address (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction.

10.2* Financial institutions should be required to maintain records of the identification data, account files and business correspondence for at least five years following the termination of an account or business relationship (or longer if requested by a competent authority in specific cases upon proper authority).

10.3* Financial institutions should be required to ensure that all customer and transaction records and information are available on a timely basis to domestic competent authorities upon appropriate authority.

[29] In the insurance sector, the word « transactions » should be understood to refer to the insurance product itself, the premium payment and the benefits. For specific requirements with regard to record keeping of transactions in the insurance sector, see the IAIS Guidance Notes of January 2002.

## Recommendation 11

The criteria listed below should be read in conjunction with the text of Recommendation 11 and its Interpretative Note.

### Essential criteria

11.1 Financial institutions should be required to pay special attention to all complex, unusual large transactions[30], or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose.

> Examples of such transactions or patterns of transactions include: significant transactions relative to a relationship, transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance, or transactions which fall out of the regular pattern of the account's activity.

11.2 Financial institutions should be required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing.

11.3 Financial institutions should be required to keep such findings available for competent authorities and auditors for at least five years.

[30] In the insurance sector, the word « transactions » should be understood to refer to the insurance product itself, the premium payment and the benefits.

**Recommendation 12**

The criteria listed below should be read in conjunction with the text of Recommendation 12, the Interpretative Note to R.5, 12 & 16, and the Criteria for Recommendations 5, 6 and 8-11.

**Essential criteria**

12.1 DNFBP should be required to comply with the requirements set out in Recommendation 5 (Criteria 5.1 – 5.17) in the following circumstances[31]:

a) Casinos (including internet casinos) – when their customers engage in financial transactions equal to or above USD/€ 3,000[32].

Examples of such financial transactions include: the purchase of casinos chips or tokens, the opening of accounts, wire transfers and currency exchanges.

b) Real estate agents – when they are involved in transactions for a 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 USD/€ 15,000[32].

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for a client in relation to the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets[33];
- management of bank, savings or securities accounts[33];
- 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 and when they carry out transactions for a client in relation to 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;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

[31] The designated thresholds applied in these criteria are referred to in the IN of R. 5, 12 and 16

[32] The designated thresholds of USD/€ 3,000 and USD/€ 15,000 include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

[33] Where the lawyer, notary, other independent legal professional or accountant is conducting financial activity as a business and meets the definition of "financial institution" then that person or firm should comply with the requirements applicable to financial institutions.

DNFBP should especially comply with the CDD measures set out in Criteria 5.3 to 5.6 but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction.

12.2 In the circumstances set out in Criteria 12.1, DNFBP should be required to comply with the criteria set out under Recommendations 6 and 8-11.

*[DG to review in line with issues raised by the Secretariat. Issue of sanctions]*

*Reporting of Suspicious Transactions and Compliance*

## Recommendation 13

The criteria listed below should be read in conjunction with the text of Recommendation 1, Recommendation 13 and its Interpretative Note, and the text of Special Recommendation IV. (Note to assessors: Ensure that the assessments of Criteria 13.1 – 13.4 and Criteria IV.1 – IV.2 (in SR.IV) are consistent.)

### Essential criteria

13.1* A financial institution should be required by law or regulation to report to the FIU (a suspicious transaction report – STR) when it suspects or has reasonable grounds to suspect[34] that funds[35] are the proceeds[36] of a criminal activity. At a minimum, the obligation to make a STR should apply to funds that are the proceeds of all offences that are required to be included as predicate offences under Recommendation 1. This 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 ML offence or otherwise (so called "indirect reporting"), is not acceptable.

13.2* The obligation to make a STR also applies to funds where there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism.

13.3* All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

13.4* The requirement to report suspicious transactions should apply regardless of whether they are thought, among other things, to involve tax matters.

### Additional criteria

13.5. Countries should consider requiring financial institutions to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction. (Note: the Interpretative Note strongly encourages countries to do this).

---

[34] The requirement to report when the individual "suspects" is a subjective test of suspicion i.e. the person actually suspected that a transaction involved a criminal activity. A requirement to report when there are "reasonable grounds to suspect" is an objective test of suspicion and can be satisfied if the circumstances surrounding the transaction would lead a reasonable person to suspect that the transaction involved a criminal activity. This requirement implies that countries may choose either the two alternatives, but need not have both.

[35] *Funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable and legal documents or instruments evidencing title to, or interest in, such assets.

[36] *Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.

## Recommendation 14

The criteria listed below should be read in conjunction with the text of Recommendation 14 and its Interpretative Note.

### Essential criteria

14.1. Financial institutions and their directors, officers and employees (permanent and temporary) 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.

14.2. Financial institutions and their directors, officers and employees (permanent and temporary) should be prohibited by law from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU.

### Additional criteria

14.3. Countries should consider enacting laws or regulations or taking other measures, consistent with the principles of domestic laws that will ensure that the names and personal details of staff of financial institutions that make a STR are kept confidential by the FIU.

**Recommendation 15**

The criteria listed below should be read in conjunction with the text of Recommendation 15, its Interpretative Note, and the definitions of "legal arrangements" and "legal persons" in the Glossary.

**Essential criteria**

The type and extent of measures to be taken for each of the requirements set out below should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

15.1 Financial institutions should be required to establish and maintain internal procedures, policies and controls to prevent ML and FT, and to communicate these to their employees. These procedures, policies and controls should cover, *inter alia,* CDD, record retention, the detection of unusual and suspicious transactions and the reporting obligation, [and should extend to foreign branches and majority owned subsidiaries. ]

15.1.1 Financial institutions should be required to develop appropriate compliance management arrangements e.g. for financial institutions at a minimum the designation of an AML/CFT compliance officer at the management level.

15.1.2 The AML/CFT compliance officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

15.2 Financial institutions should be required to maintain an adequately resourced and independent audit function to test compliance (including sample testing) with these procedures, policies and controls.

15.3 Financial institutions should be required to establish ongoing employee training to ensure that employees are kept informed of new developments, including information on current ML and FT techniques, methods and trends; and that there is a clear explanation of all aspects of AML/CFT laws and obligations, and in particular, requirements concerning CDD and suspicious transaction reporting.

15.4. Financial institutions should be required to put in place screening procedures to ensure high standards when hiring employees.

**Additional criteria**

15.5. The AML/CFT compliance officer at the management level should able to act independently and to report to the board of directors.

## Recommendation 16

The criteria listed below should be read in conjunction with the text of Recommendation 16 and its Interpretative Note, Recommendations 13-15 and their Interpretative Notes and criteria, Special Recommendation IV, and the definitions of "designated non-financial businesses and professions", "designated threshold", "FIU" and "STR". (Note to assessors: Ensure that the assessments of Criteria 16.1 – 16.3 and Criteria IV.1 – IV.3 (in SR.IV) are consistent.)

### Essential criteria

16.1 DNFBP should be required to comply with the requirements set out in Recommendation 13 (Criteria 13.1 – 13.4)[37] in the following circumstances:

a) Casinos (which includes internet casinos) – any transaction (as for financial institutions).
b) Real estate agents - any transaction (as for financial institutions).
c) Dealers in precious metals or stones - when they engage in any cash transaction equal to or above USD/€ 15,000[38].
d) Lawyers, notaries, other independent legal professionals and accountants - when, on behalf of or for a client, they engage in a financial transaction in relation to 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.

**Note on professional secrecy or legal professional privilege.**

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 jurisdiction 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. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

e) Trust and Company Service Providers - when they prepare for or carry out a transaction on behalf of a client, in relation to the following activities:

- acting as a formation agent of legal persons;

---

[37] DNFBP should comply with all the criteria in Recommendation 13 with two exceptions. First, dealers in precious metals and stones must comply with criteria 13.3, but would only be required to report transactions (or attempted transactions) above the cash threshold of USD/€ 15,000. Second, as detailed in criteria 16.1, countries may allow lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals to send their STR to self-regulatory organizations, and they do not always need to send STR to the FIU.

[38] The designated threshold includes situations where the transaction is carried out in a single operation or in several operations that appear to be linked (cases of "smurfing"/"structuring").

- 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;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

16.2 Where countries allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations[39] (SRO), there should be appropriate forms of co-operation between these organisations and the FIU. Each country should determine the details of how the SRO could co-operate with the FIU.

16.3 In the circumstances set out in criteria 16.1, the criteria set out under Recommendations 14, 15 and 21 should apply in relation to DNFBP.

**Additional criteria**

16.4. Countries should consider extending the reporting requirement to the rest of the professional activities of accountants, including auditing.

[16.5 Countries to consider extending the requirements in criteria 13.5 to DNFBP]

*DG to examine issue of sanctions R.17]*

[39] A SRO is a body that represents the profession, and which is made up of member professionals, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory type functions. For example, it would be normal for this body to enforce rules to ensure that high ethical and moral standards are maintained by those practicing the profession.

## *Other Measures to Deter Money Laundering and Terrorist Financing*

### Recommendation 17

The criteria listed below should be read in conjunction with the text of Recommendation 17, Special Recommendations IV, VI and VII, and the definition of "legal persons" in the Glossary. (Note to assessors: Ensure that Criteria 17.1 – 17.4 and Criterion IV.4 (in SR.IV), Criterion VI.5 (in SR.VI) and Criterion VII.9 (in SR.VII) are consistent.)

### Essential criteria

17.1 Countries should ensure that effective, proportionate and dissuasive criminal, civil or administrative sanctions are available to deal with natural or legal persons covered by the FATF Recommendations that fail to comply with national AML/CFT requirements.

17.2 Countries should designate an authority (e.g. supervisors, the self-regulatory organisations referred to in Recommendation 24 or the FIU) empowered to apply these sanctions. Different authorities may be responsible for applying sanctions depending on the nature of the requirement that was not complied with.

17.3 Sanctions should be available in relation not only to the legal persons that are financial institutions or businesses but also to their directors and senior management.

17.4 The range of sanctions available should be broad and proportionate to the severity of a situation. At a minimum, they should include the power to impose disciplinary and financial sanctions and the power to withdraw, restrict or suspend the financial institution's license, where applicable. [Relevant sanctions should be available for DNFBP].

> Examples of types of sanctions include: written warnings (separate letter or within an audit report), orders to comply with specific instructions (possibly accompanied with daily fines for non-compliance), criminal proceeding where permitted, 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, or controlling owners, imposing conservatorship or a suspension or withdrawal of the license.

17.5 If a natural or legal person offers financial services or operates as a casino, having failed to obtain any necessary license or registration required under national laws or regulations, that person should be subject to administrative, civil or criminal sanctions. This criterion does not require countries to create licensing or registration systems other than those required under R.24.

*[DG to review references to DNFBP in relation to other Recommendations]*

**Recommendation 18**

The criteria listed below should be read in conjunction with the text of Recommendation 18 and the definition of "shell banks" in the Glossary.

**Essential criteria**

18.1 Countries should not approve the establishment or accept the continued operation of shell banks[40].

18.2 Financial institutions should not be permitted to enter into, or continue, correspondent banking relationships with shell banks.

18.3 Financial institutions should be required to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

[40] Shell bank is defined in the Annex 2. The meaning of physical presence is not defined in these Recommendations. In its paper entitled *Shell banks and booking offices* (July 2002), the Basel Committee defines "physical presence" to be meaningful mind and management and countries should have regard to this paper.

## Recommendation 19

The criteria listed below should be read in conjunction with the text of Recommendation 19 and its Interpretative Note.

### Essential criteria

19.1 Countries should consider implementing measures to detect, monitor or report the cross-border transportation of currency and bearer negotiable instruments.

19.2 Countries should consider implementing a system to report all transactions in currency above a fixed threshold.

### Additional criteria

19.3 Where countries implement systems for reporting cross border or large currency transactions, those reports should be maintained in a computerised data base, available to competent authorities for AML/CFT purposes.

19.4 Any systems for reporting cross border or large currency transactions should be subject to strict safeguards to ensure proper use of the information or data that is reported or recorded.

19.5 Any systems for reporting cross border transactions should not impede in any way the freedom of capital movements.

19.6 If a country discovers an unusual international shipment of currency, monetary instruments, precious metals, or gems, etc., it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which the shipment originated and/or to which it is destined, and should co-operate with a view toward establishing the source, destination, and purpose of such shipment and toward the taking of appropriate action.

## Recommendation 20

The criteria listed below should be read in conjunction with the text of Recommendation 20.

### Essential criteria

20.1 Countries should consider applying Recommendations 5, 6, 8-11, 13-15, 17 and 21 to non-financial businesses and professions (other than DNFBP) that are at risk of being misused for money laundering or terrorist financing.

> Examples of businesses or professions that may be at risk include: dealers in high value and luxury goods, pawnshops, gambling, auction houses, [tax] and investment advisers.

20.2 Countries should take measures to encourage the development and use of modern and secure techniques for conducting financial transactions that are less vulnerable to money laundering.

> Examples of techniques or measures that may be less vulnerable include:
>
> - Not issuing very large denomination banknotes;
> - Ensuring that an audit trail exists for all financial transactions.

## Recommendation 21

The criteria listed below should be read in conjunction with the text of Recommendation 21.

### Essential criteria

21.1 Financial institutions should be required to give special attention to business relationships and transactions with persons (including legal entities and other financial institutions) from or in countries that do not have adequate systems in place to prevent or deter ML or FT, in line with the FATF Recommendations.

21.1.1 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.

21.2 If those transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined, and written findings should be available to assist competent authorities (e.g. supervisors, law enforcement agencies and the FIU) and auditors.

21.3 Where a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate counter-measures.

Examples of possible counter-measures include:

- Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries;
- Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;
- In considering requests for approving the establishment in FATF member countries of subsidiaries or branches or representative offices of financial institutions, taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems;
- Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of money laundering.
- Limiting business relationships or financial transactions with the identified country or persons in that country.

## Recommendation 22

The criteria listed below should be read in conjunction with the text of Recommendation 22.

### Essential criteria

*[DG to review]*

22.1 Financial institutions should be required to ensure that their foreign branches and subsidiaries[41] observe AML/CFT measures consistent with home country requirements and the FATF Recommendations, to the extent that local laws and regulations permit.

22.1.1 Financial institutions should be required to pay particular attention that this principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply the FATF Recommendations.

22.2 Where the minimum AML/CFT requirements of the home and host jurisdictions differ, branches and subsidiaries in host jurisdictions should be required to apply the higher standard, to the extent that local laws and regulations permit.

22.3 Financial institutions should be required to inform their home jurisdiction supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local laws, regulations or other measures.

[41] Subsidiaries refers to majority owned subsidiaries

## Recommendation 23

The criteria listed below should be read in conjunction with the text of Recommendation 23, its Interpretative Note, the text of Special Recommendation VI, its Interpretative Note and the definition of "Core Principles".

### Essential criteria

23.1 Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations.

23.2 Countries should ensure that a designated competent authority or authorities has/have responsibility for ensuring that financial institutions adequately comply with the requirements to combat money laundering and terrorist financing.

23.3 Supervisors or other 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, including in the executive or supervisory boards, councils, etc in a financial institution.

23.3.1 Directors and senior management of financial institutions subject to the Core Principles should be evaluated on the basis of "fit and proper" criteria including those relating to expertise and integrity.

23.4 For financial institutions that are subject to the Core Principles[42] the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes, except where specific criteria address the same issue in this Methodology.

> Examples of regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, include requirements for: (i) licensing and structure; (ii) risk management processes to identify, measure, monitor and control material risks; (iii) ongoing supervision (e.g. supervisors should have regular contact with bank management and a thorough understanding of the institution's operations) and (iv) cross-border activities (supervisors should practice global consolidated supervision over internationally-active institutions).

23.5 Businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered.

23.6 Businesses providing a service of money or value transfer, or of money or currency changing should be subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

23.7 Financial institutions (other than those mentioned in Criteria 23.4) should be licensed or registered and appropriately regulated, and subject to supervision or oversight for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector i.e. if there is a proven low risk then the required measures may be less.

*[DG ensure consistency with SRVI]*

---

[42] Note to assessors: Refer to the Core Principles for a precise description of the financial institutions that are covered, but broadly speaking it refers to: (1) banking and other deposit-taking business, (2) insurers and insurance intermediaries, and (3) collective investment schemes and market intermediaries.

**Recommendation 24**

The criteria listed below should be read in conjunction with the text of Recommendation 24.

**Essential criteria**

*[Nexus for internet casinos. Also consider the issue in Rec. 12 & 16]*

24.1 Countries should ensure that casinos (including Internet casinos) are subject to a comprehensive regulatory and supervisory regime and are effectively implementing the AML/CFT measures required under the FATF Recommendations.

24.1.1 Countries should ensure that a designated competent authority has responsibility for the regulatory and supervisory regime.

24.1.2 Casinos should be licensed by a designated competent authority.

24.1.3 A competent authority 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.

24.2 Countries should ensure that the other categories of DNFBP are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining whether the system for monitoring and ensuring compliance is appropriate, regard may be had to the risk of money laundering or terrorist financing in that sector i.e. if there is a proven low risk then the extent of the required measures may be less.

[24.2.1 There should be a designated competent authority or SRO responsible for monitoring and ensuring compliance of DNFBPs with AML/CFT requirements. Such an authority or SRO should:

a) have adequate powers to perform its functions, including powers of inspection and sanction[43];
b) have sufficient technical and other resources to perform its functions[44];
c) be able to co-operate domestically with other competent authorities[45].]

*[DG to review]*

[43] [In assessing compliance with this criterion, assessors should have regard to Criteria 29.1 to 29.5 where it is appropriate to do so (i.e. depending on the type of the designated competent authority or SRO, its size, its responsibilities, etc). ]

[44] In assessing compliance with this criterion, assessors should have regard to Criteria 30.1 to 30.6 where it is appropriate to do so (i.e. depending on the type of the designated competent authority or SRO, its size, its responsibilities, etc).

[45] In assessing compliance with this criterion, assessors should have regard to Criteria 31.1 to 31.3 where this is appropriate (i.e. depending on the type of the designated competent authority or SRO, its size, its responsibilities, etc).

## Recommendation 25

The criteria listed below should be read in conjunction with the text of Recommendation 25 and its Interpretative Note.

### Essential criteria

25.1. Competent authorities should establish guidelines that will assist financial institutions, DNFBP and any other business or profession covered by national measures, to implement and comply with national AML/CFT requirements.

> The guidelines should cover relevant aspects of the national AML/CFT system, and at a minimum should give assistance on issues covered under the relevant FATF Recommendations, including: (i) a description of ML and FT techniques, methods and trends; (ii) an explanation of the AML/CFT laws and requirements that apply; and guidance on how a financial institution, a DNFBP or other business or profession could comply with those laws and requirements; (iii) best practice measures that these institutions, businesses or professions could take to ensure that their AML/CFT measures are effective.

25.2. Competent authorities, and particularly the FIU, should provide financial institutions, DNFBP and any other business or profession that are required to report suspicious transactions, with adequate and appropriate feedback having regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.

> Examples of appropriate feedback mechanisms (drawn from the Best Practices Paper) include:
>
> (i) general feedback - (a) statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures; (b) information on current techniques, methods and trends (typologies); and (c) sanitised examples of actual money laundering cases.
>
> (ii) specific or case by case feedback - (a) acknowledgement of the receipt of the report; (b) if a case is closed or completed, whether because of a concluded prosecution, because the report was found to relate to a legitimate transaction or for other reasons, and if the information is available, then the institution should receive information on that decision or result.

## C. INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

*Competent Authorities, their Powers and Resources*

**Recommendation 26**

The criteria listed below should be read in conjunction with the text of Recommendation 26, its Interpretative Note and the definitions of "FIU" and "STR" in the Glossary.

**Essential criteria**

26.1. Countries should establish an FIU that serves as a national centre for receiving (and if permitted, requesting), analysing, and disseminating disclosures of STR and other relevant information concerning suspected ML or FT activities. The FIU can be established either as an independent governmental authority or within an existing authority or authorities.

26.2 The FIU or another competent authority should provide financial institutions and other reporting parties with guidance regarding the manner of reporting, including the specification of reporting forms, and the procedures that should be followed when reporting.

26.3 The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information and any additional information that it requires to properly undertake its functions, including the analysis of STR.

26.4 The FIU, either directly or through another competent authority, should be authorised to obtain from reporting parties additional information needed to properly undertake its functions.

26.5 The FIU should be authorised to disseminate financial information to domestic authorities for investigation or action when there are grounds to suspect ML or FT.

26.6 The FIU should have sufficient operational independence and autonomy to ensure that it is free from undue outside influence or interference.

26.7 Information held by the FIU should be securely protected and disseminated only in accordance with the law.

26.8 The FIU should publish, including electronically, periodic reports, including statistics, typologies and trends [regarding its activities].
*[DG to review]*

26.9 Where a country has created an FIU, it should consider applying for membership in the Egmont Group.

**Additional criteria**

26.10 Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.

## Recommendation 27

The criteria listed below should be read in conjunction with the text of Recommendation 27, its Interpretative Note and the definitions of "FIU" and "STR" in the Glossary.

### Essential criteria

27.1 There should be designated law enforcement[46] authorities that have responsibility for ensuring that ML and FT offences are properly investigated.

### Additional criteria

27.2 Countries should consider taking measures, whether legislative or otherwise, that will allow their law enforcement or prosecution authorities to have an adequate legal basis for the use of a wide range of special investigative techniques when conducting investigations of ML or FT, such as controlled delivery of the proceeds of crime or funds intended for use in terrorism, undercover operations, etc.

27.3 Where special investigative techniques are permitted, countries should consider developing and supporting the use of such techniques when conducting investigations of ML, FT, and underlying predicate offences. (Note: the Interpretative Note encourages countries to do this)

27.4 Countries should consider using other effective mechanisms such as the use of:

(a) Permanent or temporary groups specialised in investigating the proceeds of crime (financial investigators). An important component of the work of such groups or bodies would be focused on the investigation, seizure, freezing and confiscation of the proceeds of crime.

(b) Co-operative investigations with appropriate competent authorities in other countries, including the use of special investigative techniques, provided that adequate safeguards are in place.

(Note: the Interpretative Note encourages countries to use these mechanisms)

27.5 ML and FT methods, techniques and trends should be reviewed by law enforcement authorities, the FIU and other competent authorities (as appropriate) on a regular, interagency basis, and resulting information, analysis or studies should be disseminated to law enforcement and FIU staff, as well as staff of other competent authorities.

---

[46] In certain countries, this responsibility also rests with prosecution authorities.

## Recommendation 28

The criteria listed below should be read in conjunction with the text of Recommendation 28.

### Essential criteria

28.1 Competent authorities responsible for conducting investigations of ML, FT and other underlying predicate offences should have the powers to be able to:

a) compel production of,
b) search persons or premises for, and
c) seize and obtain

transaction records, identification data obtained through the CDD process, account files and business correspondence, and other records, documents or information, held or maintained by financial institutions and other businesses or persons. Such powers should be exercised through lawful process (for example, subpoenas, summonses, search and seizure warrants, or court orders) and be available for use in investigations and prosecutions of ML, FT, and other underlying predicate offences, or in related actions e.g. actions to freeze and confiscate the proceeds of crime.

28.2 The competent authorities referred to above should have the powers to be able to take witnesses' statements for use in investigations and prosecutions of ML, FT, and other underlying predicate offences, or in related actions.

## Recommendation 29

The criteria listed below should be read in conjunction with the text of Recommendation 29 and the definition of "supervisors" in the Glossary.

### Essential criteria

29.1 Supervisors should have adequate powers to monitor and ensure compliance by financial institutions, [including their foreign branches and majority-owned subsidiaries,] with requirements to combat money laundering and terrorist financing, consistent with the FATF Recommendations. *[DG to review issue of materiality and prohibition by local laws]*

29.2 Supervisors should [have the authority to] conduct inspections of financial institutions, including on-site inspections, to ensure compliance. Such inspections should include the review of policies, procedures, books and records, and should extend to sample testing. *[DG to review issue of effectiveness]*

29.3 Supervisors should have the power to compel production of or to obtain access to all records, documents or information relevant to monitoring compliance. This includes all documents or information related to accounts or other business relationships, or transactions, including any analysis the financial institution has made to detect unusual or suspicious transactions.

29.3.1 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.

29.4 The supervisor should have adequate powers of enforcement and sanction against financial institutions, and their directors or senior management for failure to comply with or properly implement requirements to combat money laundering and terrorist financing, consistent with the FATF Recommendations, including the power to withdraw or suspend the institution's license (see also R.17)

**Recommendation 30**

The criteria listed below should be read in conjunction with the text of Recommendation 30.

**Essential Criteria**

30.1 FIUs, law enforcement and prosecution agencies, supervisors and other competent authorities involved in combating money laundering and terrorist financing should be adequately structured, funded, staffed, and provided with sufficient technical and other resources to fully and effectively perform their functions. Adequate structuring includes the need for sufficient operational independence and autonomy to ensure freedom from undue outside influence or interference.

30.2 Staff of competent authorities should be required to maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

30.3 Staff of competent authorities should be provided with adequate and relevant training:

a) for combating ML and FT;

Adequate and relevant training should, in particular, concern the scope of predicate offences, ML and FT typologies, techniques to investigate and prosecute these offences, techniques for tracing property that is the proceeds of crime or is to be used to finance terrorism, and ensuring that such property is seized, frozen and confiscated, and the techniques to be used by supervisors to ensure that financial institutions are complying with their obligations.

b) for using information technology and other resources relevant to the execution of their functions.

30.3.1 Countries should provide special training and/or certification for financial investigators for, *inter alia*, investigations of ML, FT, and the predicate offences.

**Additional Criteria**

30.4 Countries should consider providing special training or educational programmes for judges and courts concerning ML and FT offences, and the seizure, freezing and confiscation of property that is the proceeds of crime or is to be used to finance terrorism.

## Recommendation 31

The criteria listed below should be read in conjunction with the text of Recommendation 31.

### Essential Criteria

31.1 Policy makers, the FIU, law enforcement and supervisors and other competent authorities should have effective mechanisms in place which enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

Such mechanisms should normally address:

(a) operational co-operation and, where appropriate, co-ordination between authorities at the law enforcement/FIU level (including customs authorities where appropriate); and between the FIU, law enforcement and supervisors;
(b) policy co-operation and, where appropriate, co-ordination across all relevant competent authorities,.

### Additional Criteria

31.2 Countries should have mechanisms for consultation between competent authorities, the financial sector and other sectors (including DNFBP) that are subject to AML/CFT laws, regulations, guidelines or other measures.

## Recommendation 32

The criteria listed below should be read in conjunction with the text of Recommendation 32.

## Essential Criteria

32.1 Countries should review the effectiveness of their systems for combating money laundering and terrorist financing on a regular basis.

32.2 Competent authorities should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of systems for combating money laundering and terrorist financing. This should include keeping annual statistics on:

(a) suspicious transaction reports (and other reports where appropriate under domestic law) received and disseminated -

- STR received by the FIU, including a breakdown of the type of financial institution, DNFBP, or other business or person making the STR;
- Breakdown of STR analysed and disseminated;
- Reports filed on: (i) domestic or foreign currency transactions above a certain threshold, (ii) cross border transportation of currency and bearer negotiable instruments, [(iii) international wire transfers, or (iv) other transactions related to ML or FT (only where the reporting of such transactions or transportation is required by domestic law).]

(b) ML & FT investigations; prosecutions and convictions, and on property frozen; seized and confiscated -

- ML and FT investigations, prosecutions, and convictions;
- [Any criminal, civil, or administrative sanctions applied to persons convicted of such offences;]
- The number of cases and the amounts of property frozen, seized, and confiscated relating to (i) ML,(ii) FT, and (iii) underlying predicate offences; and
- Number of persons or entities and the amounts of property frozen pursuant to or under U.N. Resolutions relating to terrorist financing.

(c) Mutual legal assistance or other international requests for co-operation -

- All mutual legal assistance and extradition requests (including requests relating to freezing, seizing and confiscation) that are made or received, relating to ML, the predicate offences and FT, including the nature and result of the request, and the time required to respond;
- Other requests for assistance made or received by the FIU, including the result of the request;
- Other requests for assistance made or received by law enforcement authorities relating to ML or FT, including the result of the request; and
- Spontaneous referrals made by the FIU to foreign authorities

(d) Other action

- On-site examinations conducted by supervisors relating to or including AML/CFT and the results of those examinations.
- Requests for assistance made or received by supervisors relating to or including AML/CFT, including the result of the request.

### Additional criteria

32.3 Competent authorities should consider maintaining comprehensive statistics on STR resulting in investigation, prosecution, or convictions for ML, FT or an underlying predicate offence.

**Recommendation 33**

The criteria listed below should be read in conjunction with the texts of Recommendation 33, and the definitions of "beneficial owner" and "legal persons".

*[Delete footnotes that are in the annex]*

**Essential criteria**

33.1 Countries should take measures to prevent the unlawful use of legal persons[47] in relation to money laundering and terrorist financing by ensuring that their commercial, corporate and other laws require adequate transparency concerning the beneficial ownership and control of legal persons.

*[Ex. Box. DG to review. Check consistency with the OECD Report]*

Examples of mechanisms that countries could use to ensure that there is adequate transparency:

1. A system of central registration where a national registry records the required ownership and control details for all companies and other legal persons registered in that country. The relevant information could be either publicly available or only available to competent authorities. Changes in ownership and control information would need to be kept up to date.

2. Requiring company service providers to obtain, verify and retain records of the beneficial ownership and control of legal persons.

3. Requiring companies and other legal persons to obtain and record the required information, to keep it within the country, and to rely on the investigative and other powers of law enforcement, regulatory or other competent authorities to obtain or have access to the information.

Countries may use a combination of the mechanisms described above.

Whatever mechanism is used it is essential that competent authorities: (a) are able to obtain or have access in a timely fashion to the beneficial ownership and control information, and (b) that the information must be adequate, accurate and timely (see Criterion 33.2).

33.2 Competent authorities should be able to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons.

33.2.1 Competent authorities should be able to share information on the beneficial ownership and control of legal persons with foreign competent authorities (in accordance with the criteria set out in R.36 & 40).

33.3 Countries that have legal persons able to issue bearer shares[48] should take appropriate measures to ensure that they are not misused for money laundering, and that the principles set out in criteria 33.1 and 33.2 above apply equally to legal persons that use bearer shares. The measures to be taken may vary from country to country, but each country should be able to demonstrate the adequacy and effectiveness of the measures that are applied.

Additional criteria

[47] "Legal persons" refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

[48] "Bearer shares" refers to negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate.

33.4 Countries could consider adopting measures to facilitate access by financial institutions to beneficial ownership and control information, so as to allow them to more easily verify the customer identification data.

**Recommendation 34**

The criteria listed below should be read in conjunction with the texts of Recommendation 34 and the definitions of "beneficial owner" and "legal arrangements".

*[Delete footnotes that are already in the annex]*

**Essential criteria**

34.1 Countries should take measures to prevent the unlawful use of legal arrangements[49] in relation to money laundering and terrorist financing by ensuring that its commercial, trust and other laws require adequate transparency concerning the beneficial ownership and control of trusts and other legal arrangements.

*[Ex. Box. DG to review. Check consistency with the OECD Report]*

Examples of mechanisms that countries could use to ensure that there is adequate transparency:

1. A system of central registration where a national registry records details on trusts (i.e. settlors, trustees, beneficiaries and protectors) and other legal arrangements registered in that country. The relevant information could be either publicly available or only available to competent authorities. Changes in ownership and control information would need to be kept up to date.

2. Requiring trust service providers to obtain, verify and retain records of the details of the trust or other similar legal arrangements.

3. Requiring trustees to obtain, verify and retain records of the required information, to keep it within the country, and to rely on the investigative and other powers of law enforcement, regulatory or other competent authorities to obtain or have access to the information.

Whatever mechanism is used it is essential that competent authorities: (a) are able to obtain or have access in a timely fashion to the beneficial ownership and control information, and (b) that the information must be adequate, accurate and timely (see Criterion 34.2).

34.2 Competent authorities should be able to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal arrangements, and in particular the settlor[50], the trustee[51] and the beneficiaries[52] of express trusts[53].

---

[49] "Legal arrangements" refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.

[50] The settlors are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.

[51] The trustees, who may be paid professionals or companies or unpaid persons, hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes. There may also be a protector, who may have power to veto the trustees' proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.

[52] All trusts (other than charitable or statutory permitted non-charitable trusts) must have beneficiaries, who may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.

53 "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. Express trusts 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.

34.2.1 Competent authorities should be able to share information on the beneficial ownership and control of legal arrangements with foreign competent authorities in accordance with the criteria set out in R.36 & 40.

**Additional criteria**

34.3 Countries could consider adopting measures to facilitate access by financial institutions to beneficial ownership and control information, so as to allow them to more easily verify the customer identification data.

## D. INTERNATIONAL CO-OPERATION

**Recommendation 35**

The criteria listed below should be read in conjunction with the texts of Recommendation 35 and Special Recommendation I, and the text of the Conventions referred to in Recommendation 35[54] (Note to assessors: Ensure that the assessments of Criterion 35.1 and Criterion I.1 (in SR.I) are consistent.)

**Essential criteria**

35.1 Countries should sign and ratify, or otherwise become a party to, and fully implement, the Vienna Convention, the Palermo Convention and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention).[55]

**Additional criteria**

35.2 Countries should consider signing, ratifying, or otherwise becoming a party to, and fully implementing other relevant international conventions such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

[54] Assessors should be satisfied that all the articles relevant to ML and FT are fully implemented.

[55] Assessors should be satisfied that the following relevant articles of the Vienna Convention (Articles 3-9), the Palermo Convention (Articles 6-7, 10-16, 18-20, 26-27, 31 and 34), and the Terrorist Financing Convention (Articles 2-18) are fully implemented.

## Recommendation 36

The criteria listed below should be read in conjunction with the text of Recommendation 36 and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criteria 36.1 – 36.6 and Criterion V.1 (in SR.V) are consistent.)

### Essential criteria

36.1 Countries should be able to provide the widest possible range of mutual legal assistance in AML/CFT investigations, prosecutions and related proceedings[56].

Mutual legal assistance includes assistance of the following nature: (i) the production or seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons; (ii) searches and seizures of financial institutions, other entities, and domiciles; (iii) the taking of evidence or statements from persons; (iv) effecting service of judicial documents; (v) providing originals or copies of relevant documents and records; and (vi) identification, freezing, seizure, or confiscation of assets laundered or intended to be laundered, the proceeds of ML and assets used for or intended to be used for FT, as well as the instrumentalities of such offences, and assets of corresponding value.

*[DG to review if minimum elements of MLA]*

36.1.1 There should be evidence (including statistics) of such assistance having been provided in a rapid, constructive and effective manner.

36.2 Mutual legal assistance should not be prohibited or made subject to unreasonable, disproportionate or unduly restrictive conditions.

Possible examples of such conditions (for which an assessment as to reasonableness, proportionality or restrictiveness should be made) could include: generally refusing to provide assistance on the grounds that judicial proceedings have not commenced in the requesting country; requiring a conviction before providing assistance; requiring a treaty before providing assistance.

36.3 There should be clear and efficient processes for the execution of mutual legal assistance requests.

Obstacles to an efficient execution of mutual legal assistance requests include: failure to take the appropriate measures in a timely way, and long delays in responding.

*[DG to consider if examples or unacceptable measures]*

36.4 A request for mutual legal assistance should not be refused on the sole ground that the offence is also considered to involve fiscal matters.

36.5 A request for mutual legal assistance should not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions [or DNFBP, except where the relevant information was obtained in circumstances where professional secrecy or legal professional privilege applies[57].] *[DG to consider references to DNFBP]*

---

[56] Investigations, prosecutions and related proceedings may be of a criminal, civil enforcement or administrative nature, and includes proceedings in relation to confiscation or provisional measures.

[57] See also Criteria 16.2

36.6 The powers of competent authorities required under R.28 should also be available for use in response to requests for mutual legal assistance.

**Additional criteria**

36.7 To avoid conflicts of jurisdiction, countries should consider 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.

36.8 Where this is consistent with the domestic framework, the powers of competent authorities required under R.28 should also be available for use when there is a direct request from foreign judicial or law enforcement authorities to domestic counterparts[58].

[58] "Counterparts" refers to the definition provided in criteria 40.1

## Recommendation 37

The criteria listed below should be read in conjunction with the text of Recommendation 37 and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criterion 37.1 and Criterion V.2 (in SR.V) are consistent.)

### Essential criteria

37.1 To the greatest extent possible, mutual legal assistance should be rendered in the absence of dual criminality, [in particular, for less intrusive and non compulsory measures.]

37.2 For extradition and those forms of mutual legal assistance where dual criminality is required, the requested state (that is rendering the assistance) should have no legal or practical impediment to rendering assistance where both countries criminalise the conduct underlying the offence. Technical differences between the laws in the requesting and requested states, such as differences in the manner in which each country categorises or denominates the offence should not pose an impediment to the provision of mutual legal assistance.

**Recommendation 38**

The criteria listed below should be read in conjunction with the text of Recommendation 38 and its Interpretative Note, and the text of Recommendation 3 and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criteria 38.1 – 38.3 and Criterion V.3 are consistent.)

**Essential criteria**

38.1 There should be appropriate laws and procedures to provide an effective and timely response to mutual legal assistance requests by foreign countries related to the identification, freezing, seizure, or confiscation of:

(a) laundered property from,
(b) proceeds from,
(c) instrumentalities used in, or
(d) instrumentalities intended for use in,

the commission of any ML, FT or other predicate offences.

38.2 The requirements in Criteria 38.1 should also be met where the request relates to property of corresponding value.

38.3 Countries should have arrangements for co-ordinating seizure and forfeiture actions with other countries.

**Additional criteria**

38.4 Countries should consider including authorising the sharing of confiscated assets between them when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

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

## Recommendation 39

The criteria listed below should be read in conjunction with the text of Recommendation 39.

### Essential criteria

39.1 Money laundering should be an extraditable offence. There should be laws and procedures to extradite individuals charged with a money laundering offence.

39.2 Countries should either:

a) extradite their own nationals or,
b) where a country does not extradite its own nationals 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. In such cases, the competent 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.

39.3 In cases where the extradition takes place and in cases where a country prosecutes its own national for offences committed in another country, countries should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of the prosecution.

39.4 Consistent with the principles of domestic law, countries should adopt measures or procedures that will allow extradition requests and proceedings relating to ML to be handled without undue delay.

### Additional criteria

39.5 Countries [should] consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

## Recommendation 40

The criteria listed below should be read in conjunction with the text of Recommendation 40 and its Interpretative Note, and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criteria 40.1 – 40.9 and Criterion V.5 (in SR.V) are consistent.)

### Essential criteria

40.1 Countries should ensure that their competent authorities[59] are able to provide the widest range of international cooperation to their foreign counterparts[60].

40.1.1 There should be evidence [(including statistics)] of such cooperation having been provided in a rapid, constructive and effective manner.

40.2 There should be clear and effective gateways, mechanisms or channels that will facilitate and allow for prompt and constructive exchanges of information directly between counterparts[61].

Examples of gateways, mechanisms or channels used in international cooperation and exchanges of information (other than MLA or extradition) include Bilateral or multilateral agreements or arrangements; Memorandum of Understanding (MOU); Memorandum of Agreement (MOA); Exchanges on the basis of reciprocity; and Exchanges through appropriate international or regional organisations or bodies such as Interpol or the Egmont Group of FIUs.

40.3. Such exchanges of information should be possible: (a) both spontaneously and upon request, and (b) in relation to both money laundering and the underlying predicate offences.

40.4 Countries should ensure that all their competent authorities are authorised to conduct inquiries on behalf of foreign counterparts.

40.4.1 In particular, countries should ensure that their FIU is authorised to make the following types of inquiries on behalf of foreign counterparts: (a) searching its own databases, including with respect to information related to suspicious transaction reports; (b) searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

40.5 [Countries should ensure that their law enforcement authorities; and where permitted by domestic law, other competent authorities are authorised to conduct investigations on behalf of foreign counterparts].

---

[59] "Competent authorities" refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

[60] "Foreign Counterparts" refers to the authorities in another country that exercise similar responsibilities and functions.

[61] Obstacles to a prompt and constructive exchange of information include failing to respond or take the appropriate measures in a timely way, and unreasonable delays in responding.

40.6 Exchanges of information should not be made subject to disproportionate or unduly restrictive conditions.

40.7 Requests for cooperation should not be refused on the sole ground that the request is also considered to involve fiscal matters.

40.8 Requests for cooperation should not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions [or DNFBP, except where the relevant information that is sought is held in circumstances where professional secrecy or legal professional privilege applies[62].]

40.9 Countries should establish controls and safeguards to ensure that information received by competent authorities is used only in an authorised manner. These controls and safeguards should be consistent with national provisions on privacy and data protection[63].

Information sharing may require clear agreements between competent authorities such as: the information exchanged is used only for the specific purpose for which the information was sought or provided; [information exchanged can only be disseminated to another agency or third party in a manner consistent with the terms of the request for information] [the information exchanged cannot be disseminated to another agency or third party a) without the prior consent of the authority that disclosed the information (such consent should not be unreasonably withheld and should be given in a timely manner)] and [b)] cannot be retained longer than it is necessary for the fulfilment of the purpose for which the information is to be used.

**Additional criteria**

40.10 Where permitted by fundamental domestic legal principles, the FIU should contact other competent authorities and financial institutions [or DNFBP] to obtain relevant information requested by a foreign counterpart FIU.

40.11 Countries [should consider] permitting a prompt and constructive exchange of information with non-counterparts and this co-operation may occur either directly or indirectly[64].

40.11.1 The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

[62] See also criteria 16.2

[63] This implies that, at a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving competent authority.

[64] The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority.

# EIGHT SPECIAL RECOMMENDATIONS - CRITERIA

## Special Recommendation I

The criteria listed below should be read in conjunction with the text of Special Recommendation I, Recommendation 35, Special Recommendations II, III and V, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), and the following United Nations Security Council Resolutions: S/RES/1267(1999), its successor resolutions 1333(2000), S/RES/1363(2001), S/RES/1390(2002) and S/RES/1455(2003), and S/RES/1373(2001). (Note to assessors: Ensure that the assessments of Criterion I.1 and Criterion 35.1 (in R.35) are consistent. Also ensure that the assessments of SR.I, SR.II, SR.III and SR.V are consistent.)

### Essential criteria

I.1 Countries should sign and ratify, or otherwise become a party to, and fully implement, the Terrorist Financing Convention.[65]

I.2 Countries should fully implement the United Nations Security Council Resolutions relating to the prevention and suppression of FT. These comprise S/RES/1267(1999), its successor resolutions S/RES/1333(2000), S/RES/1390(2002) and S/RES/1455(2003), S/RES/1363(2001) and S/RES/1373(2001). This requires any necessary laws / regulations or other measures to be in place and for these provisions to cover the requirements contained in those resolutions.

### Additional criteria

[I.3 Countries should consider signing, ratifying, or otherwise becoming a party to, and fully implementing other relevant international conventions such as the 2002 Inter-American Convention against Terrorism.]

[65] Assessors should be satisfied that all relevant articles of the Terrorist Financing Convention are fully implemented (Articles 2-6 and 17-18 which relate to SR.II; Article 8 which relates to SR.III; and Articles 7 and 9-18 which relate to SR.V.)

## Special Recommendation II

The criteria listed below should be read in conjunction with the text of Special Recommendation II, Special Recommendation I, Recommendations 1 and 2, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), the definitions of "terrorist act" and "terrorist organisation" in the Interpretative Note to Special Recommendation III and the definition of "funds" in Article 1 of the Terrorist Financing Convention. (Note to assessors: Ensure that the assessments of Criteria II.1 – II.3, Criterion I.1 (in SR.I) and Criteria 1.3 – 1.6 (in R.1) are consistent.)

## Essential Criteria

II.1 The financing of terrorism, terrorist acts and terrorist organisations (jointly referred to as terrorist financing or FT) should be criminalised on the basis of the Terrorist Financing Convention.[66,67] The offence of terrorist financing should extend to any funds as defined in the TF Convention[68]. *[DG to check consistency on definition of funds between SRIII and TF Convention]*

II.2 The offence of terrorist financing should be a predicate offence for money laundering.

II.3 The offence of terrorist financing should extend to situations where the person alleged to have committed the offence is in one country, but the terrorist(s), terrorist organisation(s), or place where the terrorist act(s) occurs is/are in another country.

II.4 Countries should ensure that Criteria 2.1 to 2.5 (in R.2) also apply in relation to the offence of FT.

II.5 Countries should ensure that Criterion 1.7 (in R.1) also applies in relation to the offence of FT.

---

[66] Article 2 of the Terrorist Financing Convention states:
"Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
(a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
(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 organization to do or to abstain from doing any act.

[67] [In order to comply with SR II, it is not sufficient to rely on ancillary offences that apply to terrorist offences e.g. aiding and abetting or conspiracy offences. This interpretation is consistent with the views of UNCTC experts.]

[68] Article 1 of the Terrorist Financing Convention defines *funds* as "assets 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 assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.

## Special Recommendation III

The criteria listed below should be read in conjunction with the text of Special Recommendation III, its Interpretative Note, its Best Practices Paper, Special Recommendation I, Recommendation 3, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), the following United Nations Security Council Resolutions: S/RES/1267(1999), its successor resolutions 1333(2000), S/RES/1363(2001), S/RES/1390(2002) and S/RES/1455(2003), S/RES/1373(2001) and S/RES/1452(2002), and the definitions of "confiscate", "designated person", "freeze", "funds or other assets", "seize", "S/RES/1267(1999)", "terrorist", "terrorist act", "terrorist organisation", "those who finance terrorism" and "without delay" in the Interpretative Note to SR.III. (Note to assessors: Ensure that the assessments of Criteria III.1 – III.12, Criteria I.1 – I.2 (in SR.I), Criteria VIII.2 (in SR.VIII) and Criteria 3.1 – 3.4 and Criterion 3.6 (in R.3) are consistent.)

## Essential criteria

*Freezing and, where appropriate, seizing under the relevant U.N. Resolutions:*

III.1 Countries should have effective laws and procedures to freeze terrorist funds or other assets of persons designated by the United Nations Al-Qaida and Taliban Sanctions Committee in accordance with S/RES/1267(1999)[69]. Such freezing should take place without delay and without prior notice to the designated persons involved.

III.2 A country should have effective laws and procedures to freeze terrorist funds or other assets of persons designated in the context of S/RES/1373(2001)[70]. Such freezing should take place without delay and without prior notice to the designated persons involved.

III.3 A country should have effective laws and procedures to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. Such procedures should ensure the prompt determination whether reasonable grounds or a reasonable basis exists to initiate a freezing action and the subsequent freezing of funds or other assets without delay upon determination, according to applicable national legal principles that a

---

[69] S/RES/1267(1999) and its successor resolutions—S/RES/1333(2000), S/RES/1363(2001), S/RES/1390(2002) and S/RES/1455(2003)—obligate countries to freeze without delay the funds or other assets owned or controlled by Al-Qaida, the Taliban, Usama bin Laden, or persons and entities associated with them as designated by the United Nations Al-Qaida and Taliban Sanctions Committee established pursuant to United Nations Security Council Resolution 1267(1999)., including funds derived from funds or other assets owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds or other assets are made available, directly or indirectly, for such persons' benefit, by their nationals or by any person within their territory. The Al-Qaida and Taliban Sanctions Committee is the authority responsible for designating the persons and entities that should have their funds or other assets frozen under S/RES/1267(1999) and its successor resolutions. All countries that are members of the United Nations are obligated by S/RES/1267(1999) and its successor resolutions to freeze the assets of persons and entities so designated by the Al-Qaida and Taliban Sanctions Committee.

[70] S/RES/1373(2001) obligates jurisdictions to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual jurisdiction has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective co-operation is developed among jurisdictions, jurisdictions should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. When (i) a specific notification or communication is sent and (ii) the jurisdiction 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 is a terrorist, one who finances terrorism or a terrorist organisation, the jurisdiction receiving the request must ensure that the funds or other assets of the designated person are frozen without delay.

requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that such grounds or basis for freezing exist.

III.4 The freezing actions referred to in Criteria III.1 – III.3 should extend to:

(a) funds or other assets wholly or jointly[71] owned or controlled, directly or indirectly, by designated persons, terrorists, those who finance terrorism or terrorist organisations; and

(b) funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons, terrorists, those who finance terrorism or terrorist organisations.

III.5 Countries should have effective systems for communicating actions [to be] taken under the freezing mechanisms referred to in Criteria III.1 – III.3 to the financial sector immediately upon taking such action. *[DG to consider mechanisms to communicate to the general public]*

III.6 Countries should provide clear guidance to financial institutions and other persons or entities that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms.

III.7 Countries should have effective and publicly-known procedures for considering de-listing requests and for unfreezing the funds or other assets of de-listed persons or entities in a timely manner consistent with international obligations.

III.8 Countries should have effective and publicly-known procedures for unfreezing, in a timely manner, the funds or other assets of persons or entities inadvertently affected by a freezing mechanism upon verification that the person or entity is not a designated person.

III.9 Countries should have appropriate procedures for authorising access to funds or other assets that were frozen pursuant to S/RES/1267(1999) and that have been determined to be necessary for basic expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses. These procedures should be in accordance with S/RES/1452(2002).

III.10 Countries should have appropriate procedures through which a person or entity whose funds or other assets have been frozen can challenge that measure with a view to having it reviewed by a court.

*Freezing, Seizing and Confiscation in other circumstances*

III.11 Countries should ensure that Criteria 3.1 – 3.4 and Criterion 3.6 (in R.3) also apply in relation to the freezing, seizing and confiscation of terrorist-related funds or other assets in contexts other than those described in Criteria III.1 – III.10.

*General provisions*

III.12 Laws and other measures should provide protection for the rights of bona fide third parties. Such protection should be consistent with the standards provided in Article 8 of the Terrorist Financing Convention, where applicable.

III.13 Countries should have appropriate measures to monitor effectively the compliance with relevant legislation, rules or regulations governing the obligations under SR III and to impose civil,

[71] "Jointly" refers to those assets held jointly between or among designated persons, terrorists, those who finance terrorism or terrorist organisations on the one hand, and a third party or parties on the other hand.

administrative or criminal sanctions for failure to comply with such legislation, rules or regulations.

**Additional criteria**

III.14 Countries should consider implementing the measures set out in the Best Practices Paper for SR.III.

III.15 Countries should consider implementing procedures to authorise access to funds or other assets that were frozen pursuant to S/RES/1373(2001) and that have been determined to be necessary for basic expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses. These procedures should be consistent with S/RES/1373(2001) and the spirit of S/RES/1452(2003).

## Special Recommendation IV

The criteria listed below should be read in conjunction with the texts of Special Recommendation IV, and Recommendations 13, 16 and 17. (Note to assessors: Ensure that the assessments of Criteria IV.1 – IV.4, Criteria 13.1 – 13.4 (in R.13), Criterion 16.1 – 16.3 (in R.16) and Criteria 17.1 – 17.4 (in R.17) are consistent.)

### Essential criteria

IV.1 A financial institution should be required by law or regulation to report to the FIU (a suspicious[72] transaction report – STR) when it suspects or has reasonable grounds to suspect that funds[73] are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism. This 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 FT offence or otherwise (so called "indirect reporting"), is not acceptable.

IV.2 Countries should ensure that Criteria 13.3 – 13.4 (in R.13) also apply in relation to the obligations under SR IV.

IV.3 Countries should ensure that Criteria IV.1 – IV.2 apply to DNFBP in the circumstances set out in Criterion 16.1 (in R.16), and subject to any qualifications under R.16.

IV.4 [Countries should ensure that Criteria 17.1 – 17.4 (in R.17) also apply in relation to the obligations under SR IV.
*[DG to review]*

### Additional criteria

IV.5 Countries should consider whether Criterion 16.4 should apply to DNFBP in the circumstances set out in Criterion 16.1 (in R.16), and subject to any qualifications under R.16.

---

[72] Systems based on the reporting of unusual transactions (rather than suspicious transactions) are equally satisfactory.

[73] *Funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable and legal documents or instruments evidencing title to, or interest in, such assets. (This definition of *funds* is also used in R.13.)

## Special Recommendation V

The criteria listed below should be read in conjunction with the texts of Special Recommendation V, Special Recommendation I, Recommendations 36-40, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), Special Recommendation III and the definition of "terrorist act" in the Interpretative Note to Special Recommendation III. (Note to assessors: Ensure that the assessments of Criteria V.1 – V.5, Criterion I.1 (in SR.I), Criteria 36.1 – 36.6 (in R.36), Criterion 37.1 (in R.37), Criteria 38.1 – 38.3 (in R.38) and Criteria 40.1 – 40.9 (in R.40) are consistent.)

### Essential criteria

V.1 Countries should ensure that Criteria 36.1 – 36.6 (in R.36) also apply to the obligations under SR.V.

V.2 Countries should ensure that Criterion 37.1 (in R.37) also applies to the obligations under SR.V.

V.3 Countries should ensure that Criteria 38.1 – 38.3 (in R.38) also apply to the obligations under SR.V.

V.4 Countries should ensure that Criteria 39.1 – 39.4 (in R.39) also apply to extradition proceedings related to terrorist acts and FT.

V.5 Countries should ensure that Criteria 40.1 – 40.9 (in R.40) also apply to the obligations under SR.V.

### Additional criteria

V.6 Countries should consider whether Criterion 36.7 – 36.8 (in R.36) should apply in relation to the obligations under SR.V.

V.7 Countries should consider whether Criterion 38.4 – 38.5 (in R.38) should apply in relation to the obligations under SR.V.

V.8 Countries should consider whether Criterion 39.5 (in R.39) should apply extradition proceedings related to terrorist acts or FT.

V.9 Countries should consider whether Criteria 40.10 – 40.11 (in R.40) should apply in relation to the obligations under SR.V.

## Special Recommendation VI

The criteria listed below should be read in conjunction with the text of Special Recommendation VI, its Interpretative Note and its Best Practices Paper, Special Recommendation VII and its Interpretative Note, Recommendation 17 and the definitions of "agent", "licensing", "money or value transfer service", and "registration" in the Interpretative Note to Special Recommendation VI. (Note to assessors: Ensure that the assessments of Criterion VI.5 and Criteria 17.1 – 17.4 (in R.17) are consistent.)

### Essential criteria

VI.1 Countries should designate a competent authority to register and/or licence natural and legal persons that perform money or value transfer services (MVT service operators), maintain a current list of the names and addresses of licensed and/or registered MVT service operators, and be responsible for ensuring compliance with licensing and/or registration requirements.[74]

VI.2 Countries should ensure that all MVT service operators are subject to the applicable FATF Forty Recommendations (in particular Recommendations 4-11, 13-15 and 21-23) and FATF Eight Special Recommendations (in particular SR.VII).

VI.3 Countries should have systems in place for monitoring licensed/registered MVT service operators and ensuring that they comply with the FATF Recommendations.

VI.4 Countries should require each licensed or registered MVT service operator to maintain a current list of its agents and to provide that list to the designated competent authority.

VI.5 Countries should ensure that Criteria 17.1 – 17.4 (in R.17) also apply in relation to the obligations under SR VI.

### Additional Criteria

VI.6 Countries should consider implementing the measures that are set out in the Best Practices Paper for SR VI.

[74] SR.VI does not require countries to establish a separate licensing/registration system or designate another competent authority in respect of money remitters which are already licensed/registered as financial institutions within the country, permitted to perform MVT services under the terms of their license/registration, and already subject to the full range of applicable obligations under the FATF Forty Recommendations and Eight Special Recommendations.

## Special Recommendation VII

The criteria listed below should be read in conjunction with the text of SR.VII and its Interpretative Note, Recommendations 5 and 17, and the definitions of "cross-border transfer", "domestic transfer", "financial institution", "funds transfer", "originator" and "wire transfer" in the Interpretative Note to Special Recommendation VII. (Note to assessors: Ensure that the assessments of Criterion VII.1, VII.9, Criteria 5.2 – 5.3 (in R.5) and Criteria 17.1 – 17.4 (in R.17) are consistent.)

### Essential criteria

SR VII 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 card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by SR VII, 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.

VII.1 For cross-border wire transfers (including batch transfers[75] and transactions using a credit or debit card to effect a funds transfer[76]), the ordering financial institution should be required to include the following *originator* information, verified for accuracy in accordance with Criteria 5.3 (in R.5), in the message or payment form accompanying the wire transfer:

- the name of the originator;
- the originator's account number (or a unique reference number if no account number exists); and
- the originator's address (countries may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth).

If a cross-border wire transfer is contained within a batch transfer and is sent by a financial institution, it may be treated as a domestic wire transfer. However, if it is sent through a money/value transfer service[77] (i.e. a money remitter), it must be treated as a cross-border wire transfer.

These requirements do not apply to: (a) credit or debit card transactions if the credit or debit card number accompanies all wire transfers that flow from the transaction; and (b) transfers and settlements between financial institutions where both the originator and beneficiary are financial institutions acting on their own behalf.

VII.2 For domestic wire transfers (including transactions using a credit or debit card as a payment system to effect a money transfer), the ordering financial institution should be required to comply with Criteria VII.1 above or it may include only the originator's account number or a unique identifier provided that the originator information referred to above can be made available to the

---

[75] A *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.

[76] This example relates to new products, such as those developed by Visa and Mastercard, which allow debit or credit cards to be used to effect wire transfers through a proprietary system. This example does not refer to conventional debit or credit card transfers (such as withdrawals from a bank account through an ATM machine, cash advances from a credit card, or payments for goods and services) which are exempt from SR VII.

beneficiary financial institution/competent authorities within three business days of receiving a request, and domestic law enforcement authorities can compel immediate production of it.

These requirements do not apply to: (a) credit or debit card transactions if the credit or debit card number accompanies all wire transfers that flow from the transaction; and (b) transfers and settlements between financial institutions where both the originator and beneficiary are financial institutions acting on their own behalf.

VII.3 Financial institutions should be required to ensure that only routine wire transfers are sent in batch transfers. Financial institutions should not batch wire transfers that are not routine or carry an increased risk of being related to money laundering or terrorist financing.

The following is a typical example of a routine batch transfer. Every month, Financial Institution A sends 100 wire transfers relating to pension/social security/dividend payments etc. to 100 customers of Financial Institution B. Financial Institution A sends all 100 wire transfers to Financial Institution B in a single batch rather than sending them each individually. Because of the routine nature of these wire transfers, there is little risk that they are related to ML/FT.

VII.4 Each intermediary financial institution in the payment chain should be required to maintain all the required originator information with the accompanying wire transfer.[78]

VII.5 If the country has a *de minimis* threshold in place, that threshold must not be above USD 3,000.[79] Notwithstanding any thresholds, accurate and meaningful originator information must be retained and made available by the ordering financial institution as set forth in Criterion VII.1.

VII.7 Beneficiary financial institutions should adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information.

An example of a procedure for handling such wire transfers would be to:

- Request the missing originator information from the financial institution that sent the wire transfer.
- If the missing information is not forthcoming, consider whether, in all the circumstances, the absence of complete originator information creates or contributes to suspicion about the wire transfer or a related transaction. If the wire transfer is deemed to be suspicious, then it should be reported to the FIU. In addition, the institution may decide not to accept the wire transfer.
- In appropriate circumstances, beneficiary financial institutions should consider restricting or terminating business relationships with financial institutions that do not comply with SR VII. In this regard, evaluators/assessors could also refer to the criteria for R.5 (Criteria 5.14 – 5.15).

[78]However, where technical limitations prevent the full originator information accompanying a cross border wire transfer from remaining with a related domestic wire transfer, a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution. This option is only possible until 14 February 2005.

[79] Jurisdictions may have a *de minimis* threshold (no higher than USD 3,000) [until the FATF has completed its review of the appropriateness of the threshold. The FATF will undertake such a review commencing in February 2004. Where a de minimis threshold exists in a country, assessors should examine the appropriateness of that threshold.]

VII.8 Countries should have measures in place to effectively monitor the compliance of financial institutions with rules and regulations implementing SR.VII.

VII.9 Countries should ensure that Criteria 17.1 – 17.4 (in R.17) also apply in relation to the obligations under SR.VII.

## Special Recommendation VIII

The criteria listed below should be read in conjunction with the text of Special Recommendation VIII, its Best Practices Paper, the definition of "non-profit organisation" in paragraphs 2 – 3 of the Best Practices Paper to SR.VIII, Special Recommendation III, and the definitions of "freeze", "funds or other assets", "seize", "terrorist" and "terrorist organisation" in the Interpretative Note to SR.III. (Note to assessors: Ensure that the assessments of Criterion VIII.2 and Criteria III.1 – III.13 (in SR III) are consistent.

### Essential criteria

In implementing the criteria below, countries may take a risk based approach taking into account, for example, the size of the organisation, the amount of funds it handles, and its specific objectives.

VIII.1 Countries should review the adequacy of laws and regulations that relate to non-profit organizations that can be abused for the financing of terrorism. There should be evidence available to assessors that this review has taken place.

VIII.2. Countries should have measures in place to ensure that terrorist organisations cannot pose as legitimate non-profit organisations, including for the purpose of escaping asset freezing or seizing measures.

VIII.3 Countries should have measures in place to ensure that funds or other assets collected by or transferred through non-profit organizations are not diverted to support the activities of terrorists or terrorist organisations.

Examples of possible measures (drawn from the Best Practices Paper to Special Recommendation VIII) include:

- Oversight on the non-profit sector that is flexible, effective, and proportional to the risk of abuse by terrorists
- Record-keeping and reporting policies to enhance the financial transparency of non-profit organisations
- Having an ability to verify that funds have been spent as advertised and planned
- Requiring non-profit organisations to document their administrative, managerial and policy control over their operations
- Effective coordination between non-profit sector oversight/regulatory bodies, law enforcement and security agencies, FIUs, and financial system regulators.
- Guidance to financial institutions with regard to CDD and suspicious transaction reporting where the client is an NPO.

### Additional criteria

VIII.4 Countries could consider implementing the measures set out in the Best Practices Paper for SR.VIII.

**Annex 1**

**Aide-memoire to assessors**
**Types of Financial Institutions covered by the 40+ 8 Recommendations**

*[DG to review contents and formatting. Issue of lawyers and DNFBP. Add note to assessors]*

| Financial Activity | Examples of types of financial institutions that engage in the activity |
|---|---|
| 1. Acceptance of deposits and other repayable funds from the public. | Banks, credit unions, building societies, savings and loan institutions. |
| 2. Lending. | Banks, Mortgage lending company, finance company, [factoring company] |
| 3. Financial leasing. | Leasing companies for non-consumer products |
| 4. The transfer of money or value. | Money remittance businesses (MVT service operators, both formal and informal) |
| 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). | Payment companies |
| 6. Financial guarantees and commitments. | Banks etc |
| 7. Trading in:<br>(a) money market instruments (cheques, bills, CDs, derivatives etc.);<br>(b) foreign exchange;<br>(c) exchange, interest rate and index instruments;<br>(d) transferable securities;<br>(e) commodity futures trading. | Brokers (market intermediaries) |
| 8. Participation in securities issues and the provision of financial services related to such issues. | Brokers (market intermediaries), investment banks |
| 9. Individual and collective portfolio management. | Covers management of collective investment schemes such as unit trusts, mutual funds, private pension funds |
| 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. | Custodians |
| 11. Otherwise investing, administering or managing funds or money on behalf of other persons. | Could apply to FI mentioned above, |
| 12.Underwriting and placement of life insurance and other investment related insurance. | Life insurance companies, agents and brokers. Also cover other investment linked insurance. Application to viatical settlements? [A viatical settlement is a lump sump given to terminally ill people (viators) in exchange for the death benefits of their life insurance. |
| 13.Money and currency changing. | Bureaux de change, money exchange business |

**Annex 2**

## DEFINITIONS USED IN THE METHODOLOGY - THE 40 RECOMMENDATIONS

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Beneficial owner* | *Beneficial owner* refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement. | Glossary | R.5, 6, 21, 23, 24, 33, and 34 |
| *Bearer shares* | *Bearer shares* refers to negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate. | OECD Report of April 2001 on "Using Corporate Entities for Illicit Purposes" | R.33 |
| *Competent authorities* | *Competent authorities* refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors. | IN of R.40 | Applicable to R.40 |
| *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. | Glossary | R. 23 |
| *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 of funds, cheque clearing, payable-through accounts and foreign exchange services. | | R.7 and 18 |
| *Designated categories of offences* | *Designated categories of offences* means:<br>• participation in an organised criminal group and racketeering;<br>• terrorism, including terrorist financing;<br>• trafficking in human beings and migrant smuggling;<br>• sexual exploitation, including sexual exploitation of | Glossary | R.1 |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| | children;<br>• illicit trafficking in narcotic drugs and psychotropic substances;<br>• illicit arms trafficking;<br>• illicit trafficking in stolen and other goods;<br>• corruption and bribery;<br>• fraud;<br>• counterfeiting currency;<br>• counterfeiting and piracy of products;<br>• environmental crime;<br>• murder, grievous bodily injury;<br>• kidnapping, illegal restraint and hostage-taking;<br>• robbery or theft;<br>• smuggling;<br>• extortion;<br>• forgery;<br>• piracy; and<br>• insider trading and market manipulation.<br><br>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:***<br>***a) Casinos (which also includes internet casinos).***<br>***b) Real estate agents.***<br>***c) Dealers in precious metals.***<br>***d) Dealers in precious stones.***<br>***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 measures that would combat money laundering.***<br>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:<br><br>• acting as a formation agent of legal persons;<br>• acting as (or arranging for another person to act as) a director or secretary of a company, a | Glossary | R. 4, 5, 12, 16, 17, 20, 24, 25, 31, 32, 36, 40 and SR IV |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| | partner of a partnership, or a similar position in relation to other legal persons;<br>• providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;<br>• acting as (or arranging for another person to act as) a trustee of an express trust;<br>• acting as (or arranging for another person to act as) a nominee shareholder for another person. | | |
| *Designated threshold* | *Designated threshold* refers to the amount set out in the Interpretative Notes. | Glossary | R.5, 12 and16 |
| *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 e.g. constructive trust. | | R.12, 16 and 34 |
| *Financial institutions* | *Financial institutions* means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:<br>1. Acceptance of deposits and other repayable funds from the public.[80]<br>2. Lending.[81]<br>3. Financial leasing.[82]<br>4. The transfer of money or value.[83]<br>5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).<br>6. Financial guarantees and commitments.<br>7. Trading in:<br>(a) money market instruments (cheques, bills, CDs, | Glossary | R.4-6, 11, 14-18, 21-23, 25, 26, 28-30, 33, 34, 36, 40, SRIII, SRIV, SRVI and SRVII |

[80] This also captures private banking.

[81] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).

[82] This does not extend to financial leasing arrangements in relation to consumer products.

[83] This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. 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 Interpretative Note to Special Recommendation VII.

[84] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| | derivatives etc.);<br>(b) foreign exchange;<br>(c) exchange, interest rate and index instruments;<br>(d) transferable securities;<br>(e) commodity futures trading.<br>8. Participation in securities issues and the provision of financial services related to such issues.<br>9. Individual and collective portfolio management.<br>10. Safekeeping and administration of cash or liquid securities on behalf of other persons.<br>11. Otherwise investing, administering or managing funds or money on behalf of other persons.<br>12. Underwriting and placement of life insurance and other investment related insurance[84].<br>13. Money and currency changing.<br>When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.<br>In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above. | | |
| *FIU* | FIU means financial intelligence unit. | Glossary | R.3, 13, 14, 16, 17, 21, 25-27, 30-32, 40, SRIV and SR VII |
| *Foreign counterparts* | *Foreign counterparts* refers to the authorities in another country that exercise similar responsibilities and functions. | IN of R.40 | Applicable to the criteria under R.40 |
| *Funds* | *Funds* refers to assets of every kind, [whether corporeal or incorporeal, tangible or intangible, movable or immovable and legal documents or instruments evidencing title to, or interest in, such assets]. | | R.13 and 27 |
| *Legal arrangements* | *Legal arrangements* refers to express trusts or other similar legal arrangements. Examples of other similar arrangements | Glossary. | R.5, 15 and 34 |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| | (for AML/CFT purposes) include fiducie, treuhand and fideicomiso. | | |
| *Legal persons* | *Legal persons* refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property. | Glossary | R.2, 5, 12, 15-17, 21, 33, 36 and SR VI |
| *Payable-through accounts* | *Payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf. | Glossary | R.7 |
| *Politically Exposed Persons" (PEPs)* | *PEPs* are individuals who are or have been entrusted with prominent public functions in 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. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. | Glossary | R.6 |
| *Proceeds* | *Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence. | Palermo Convention | R.1, 3, 13, 27, 28, 30, 35, 36 & 38 |
| *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. | Palermo Convention | R.1, 3, 30, 32, and 38 |
| *Self-regulatory organisation (SRO)* | A *SRO* is a body that represents the profession, and which is made up of member professionals, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory type functions. For example, it would be normal for this body to enforce rules to ensure that high ethical and moral standards are maintained by those practicing the profession. | | R.16 and 24 |
| *Settlor* | *Settlors* are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets. | | R.7 and 34 |
| *Shell bank* | *Shell bank* means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group. | Glossary | R.18 |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *STR* | *STR* refers to suspicious transaction reports. | Glossary | R.13, 14, 16, 26 & 27 and SRIV |
| *Supervisors* | *Supervisors* refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing. | Glossary | R.17, 21, 23, 29, 30-32 and 40 |
| *The FATF Recommendations* | *The FATF Recommendations* refers to these Recommendations and to the FATF Special Recommendations on Terrorist Financing. | Glossary | R.4, 5, 9, 17, 21-24, 29 and SRVI |
| *Trustee* | *Trustees*, who may be paid professionals or companies or unpaid persons, hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes. There may also be a protector, who may have power to veto the trustees' proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees. | | R. 5, 12, 16 and 34 |

**Annex 3**

## DEFINITIONS USED IN THE METHODOLOGY - THE 8 SPECIAL RECOMMENDATIONS

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Agent* | An *agent* is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires). (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.) | INSR.VI | Definitions of "DNFBP" and "financial institution", R.9, 12, 16 and SR.VI |
| *Confiscate* | The term *confiscate,* 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.) (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III.) | INSR.III | R.28, 30, 32, 38 and SR.III |
| *Cross-border transfer* | *Cross-border transfer* means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | INSR.VII |
| *Designated person* | The term *designated persons* refers to those persons or entities designated by the Al-Qaida and Taliban Sanctions Committee pursuant to S/RES/1267(1999) or those persons or entities designated and accepted, as appropriate, by jurisdictions pursuant to S/RES/1373(2001). (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III.) | INSR.III | INSR.III |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Domestic transfer* | *Domestic transfer* means any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | INSR.VII |
| *Financial institution* | The term *financial institution* is as defined by the FATF Forty Recommendations (2003). The term does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | Definition of "financial institution",<br><br>R.4-18, 21-23, 25-26, 28-30, 32-34, 36, 40, SR.III, IV, VI andVII |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Freeze* | *Freeze* means to prohibit the transfer, conversion, disposition or movement of funds or other assets 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. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the freezing and may continue to be administered by the financial institution or other arrangements designated by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III ans SR.VIII.) | INSR.III | R.3, 27-28, 30, 32, 36, 38 and SR.III and VIII |
| *Funds or other assets* | The term *funds or other assets* means financial assets, 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. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III and SR.VIII.) | INSR.III | Definition of "financial institutions",<br><br>R.5-7, 13, 27 and SR.II, III, IV, VII and VIII |
| *Funds transfer* | The terms *funds transfer* refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | SR.VII |
| *Licensing* | *Licensing* means a requirement to obtain permission from a designated competent authority in order to operate a money/value transfer service legally. (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.) | INSR.VI | R.17, 23 and SR.VI |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Money or value transfer service* | *Money or value transfer service* refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.<br><br>A money or value transfer service may be provided by persons (natural or legal) formally through the regulated financial system or informally through non-bank financial institutions or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or *underground* (or *parallel) banking systems*. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala, hundi, fei-chien,* and the *black market peso exchange*. (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.) | INSR.VI | R.23 and SR.VI |
| *Non-profit organisations* | Non-profit organisations can take on a variety of forms, depending on the jurisdiction and legal system. Within FATF members, law and practice recognise associations, foundations, fund-raising committees, community service organisations, corporations of public interest, limited companies, Public Benevolent Institutions, all as legitimate forms of non-profit organisation, just to name a few.<br><br>This variety of legal forms, as well as the adoption of a risk-based approach to the problem, militates in favour of a functional, rather than a legalistic definition. Accordingly, the FATF has developed suggested practices that would best aid authorities to protect non-profit organisations **that engage in raising or disbursing funds** for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works" from being misused or exploited by the financiers of terrorism. (This definition is drawn from the Best Practices Paper to SR.VIII. It is used in the criteria under SR.VIII.) | BPP.VIII | SR.VIII |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Originator* | The *originator* is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | SR.VII |
| *Registration* | *Registration* in this Recommendation means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally. (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.) | INSR.VI | R.17, 33, 34 and SR.VI |
| *Seize* | The term *seize* means to prohibit the transfer, conversion, disposition or movement of funds or other assets 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 funds or other assets. The seized funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized funds or other assets. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III and SR.VIII.) | INSR.III | R.3, 27-28, 30, 32, 36, 38 and SR.III and VIII |
| *S/RES/1267(1999)* | The term *S/RES/1267(1999)* refers to S/RES/1267(1999) and its successor resolutions. When issued, S/RES/1267(1999) had a time limit of one year. A series of resolutions have been issued by the United Nations Security Council (UNSC) to extend and further refine provisions of S/RES/1267(1999). By successor resolutions are meant those resolutions that extend and are directly related to the original resolution S/RES/1267(1999). As of November 2003, these resolutions included S/RES/1333(2000), S/RES/1363(2001), S/RES/1390(2002) and S/RES/1455(2003). (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.I and SR.III. It is used in the criteria under SR.III.) | INSR.III | SR.I and III |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *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 or terrorist financing; (iii) organises or directs others to commit terrorist acts or terrorist financing; or (iv) contributes to the commission of terrorist acts or terrorist financing 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 terrorist financing or with the knowledge of the intention of the group to commit a terrorist act or terrorist financing. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III and SR.VIII.) | INSR.III | SR.II, III and VIII |
| *Terrorist act* | A *terrorist act* includes an act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft, Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, International Convention against the Taking of Hostages, Convention on the Physical Protection of Nuclear Material, 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, Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, International Convention for the Suppression of Terrorist Bombings, and the International Convention for the Suppression of the Financing of Terrorism (1999). (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.II, SR.III, SR.V.) | INSR.III | R.13 and SR.II, III, IV and V |
| *Terrorist organisation* | The term *terrorist organisation* refers to any legal person, group, undertaking or other entity owned or controlled directly or indirectly by a terrorist(s). (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.II, SR.III and SR.VIII.) | INSR.III | R.13 and SR.II, III, IV and VIII |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Those who finance terrorism* | The phrase *those who finance terrorism* refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III.) | INSR.III | R.13 and SR.III and IV |
| *Without delay* | The phrase *without delay,* for the purposes of S/RES/1267(1999), means, ideally, within a matter of hours of a designation by the Al-Qaida and Taliban 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. The phrase *without delay* should be interpreted in the context of the need to prevent the flight or dissipation of terrorist-linked funds or other assets, and the need for global, concerted action to interdict and disrupt their flow swiftly. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III.) | INSR.III | R.9 and SR.III |
| *Wire transfer* | The terms *wire transfer* refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | R.5, 7, 12, 32 and SR.VII |

**NOTE:** This list does not include the following definitions which are also used in the assessment of the Eight Special Recommendations:

- *batch transfer* (as used in the criteria under SR.VII);
- *funds* (as defined in Article 1 of the Terrorist Financing Convention and used in the criteria under SR.II); or

# METHODOLOGY FOR ASSESSING COMPLIANCE WITH ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM STANDARDS 2003

## Introduction

*[DG to review status of additional criteria, the differing requirements in the FATF 40 + 8 Recommendations such as "should", "should be required", "should consider", "are encouraged" etc. Also to consider particularly §5, 10 & 11, 13, key definitions in §16, 17 & 18 (content and formatting), definition of "law or regulation and other enforceable means", implementation issue in §25, etc],*

This document consists of three sections. Following this introduction, the first section consists of an overview of the assessment methodology, its background, a description of the structure of the document, and of certain conditions that are not included in the assessment criteria but that are nevertheless necessary for an effective anti-money laundering and combating the financing of terrorism ("AML/CFT") system. The second section consists of guidance and interpretation concerning the Methodology, the criteria and compliance, and the terminology that is used. Finally, the third section sets out the AML/CFT assessment criteria themselves.

## The AML/CFT Assessment Methodology

### Background to Methodology

1. The Anti-Money Laundering/Combating Terrorist Financing (AML/CFT) Methodology 2003, including the assessment criteria, is designed to guide the assessment of a country's[1] compliance with the international AML/CFT standards as contained in the FATF Forty Recommendations 2003 and the FATF Eight Special Recommendations on Terrorist Financing 2001 (referred to jointly as the FATF Recommendations). The Methodology is a key tool to assist assessors when they are preparing AML/CFT detailed assessment reports/mutual evaluation reports.

2. It is based on the AML/CFT Methodology issued in October 2002, but is revised to take into account the significant revisions that were made in the Forty Recommendations 2003. It is also informed by the assessment experience of the FATF and the FATF-style regional bodies (FSRBs) (from their mutual evaluations), of the International Monetary Fund (the Fund) and the World Bank (the Bank)(in the Financial Sector Assessment Program (FSAP)) and by the Fund (in the Offshore Financial Center assessment program (OFC)). The FATF, the Fund and the Bank have also reviewed the assessments/mutual evaluations conducted in 2002 and 2003 using the AML/CFT Methodology issued in October 2002, and these reviews have also provided guidance in developing this Methodology.

3. [The Methodology was agreed by the FATF Plenary at its meeting in February 2004, and approved by the Executive Boards of the Fund and the Bank in March 2004. [The following FSRBs have also endorsed the Methodology: .]]

### The Structure of the Methodology Document

4. An effective AML/CFT system requires an adequate legal and institutional framework, which should include: (i) laws that create money laundering (ML) and terrorist financing (FT) offences and provide for the freezing, seizing and confiscation of the proceeds of crime and terrorist funding; (ii) laws, regulations or in certain circumstances other enforceable means that impose the required obligations on financial institutions and designated non-financial businesses and professions; (iii) an appropriate institutional or administrative framework, and laws that provide competent authorities with the necessary

[1] All references to "country" in this Methodology include territories or jurisdictions. See paragraph 16.

duties, powers and sanctions; and (iv) laws and other measures that give a country the ability to provide the widest range of international co-operation . It is also essential that the competent authorities ensure that the whole system is effectively implemented.

5. It should be noted that in some countries, 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. For example, profit generating criminal offences may exist at both federal and state levels, and thus measures to combat money laundering should be taken at the state/provincial level. When evaluations or assessments are being conducted, appropriate steps should be taken to ensure that AML/CFT measures at the state/provincial level are also adequately addressed.

6. The Methodology follows the structure of the FATF Recommendations. However, as the Methodology is a tool to assist assessors in determining whether countries are in compliance with the FATF Recommendations, it is not intended that detailed assessment reports/mutual evaluation reports will rigidly follow the format and structure of the Methodology. Rather the format for these reports will be based on the four fundamental areas noted in paragraph 4 above. The assessments will also need to be based on and refer to relevant underlying information, such as the quantum and type of predicate offences for money laundering; the vulnerability of the country to money laundering or terrorist financing, the methods, techniques and trends used to launder money or fund terrorists; the structure of the financial system and the nature of the sectors dealing with designated non-financial businesses and professions; the nature of the underlying criminal justice system, as well as any changes that have been made to the AML/CFT system in the relevant period. Most importantly, the format of the reports will allow for an assessment of whether the Recommendations have been fully and properly implemented and the AML/CFT system is effective. As in previous FATF evaluation rounds, this could be judged by reference to quantitative data and the results that have been achieved, or could be based upon more qualitative factors.

### Other factors necessary for an effective AML/CFT system

7. An effective AML/CFT system requires that certain structural elements, not covered by the AML/CFT assessment criteria, also be in place. The lack of such elements, or significant weaknesses or shortcomings in the general framework, may significantly impair the implementation of an effective AML/CFT framework. Although the AML/CFT assessment criteria do not cover these conditions, apparent major weaknesses or shortcomings identified should be noted in the mutual evaluation/detailed assessment report. These elements should include in particular:

a) sound and sustainable macro-economic policies;
b) a well-developed public sector infrastructure, having regard to the level of economic development of the country;
c) the respect of principles such as transparency and good governance;
d) a proper culture of AML/CFT deterrence shared and reinforced by government, financial institutions, designated non-financial businesses and professions; industry trade groups, and self-regulatory organisations (SROs);
e) appropriate measures to combat corruption;
f) a reasonably efficient court system that ensures that judicial decisions are properly enforced;
g) high ethical and professional requirements for police officers, prosecutors, judges, etc. and measures and mechanisms to ensure these are observed;
h) a system for ensuring the ethical and professional behaviour on the part of professionals such as accountants and auditors, and lawyers. This may include the existence of codes of conduct and good practices, as well as methods to ensure compliance such as registration, licensing, and supervision or oversight.

## Guidance on the Criteria, the Compliance ratings, and General Interpretation concerning the AML/CFT Standards and Methodology

### The Criteria and Compliance

8. The assessment of the adequacy of a country's AML/CFT framework will not be an exact process, and the vulnerabilities and risks that each country has in relation to ML and FT will be different depending on domestic and international circumstances. ML and FT techniques evolve over time, and therefore AML/CFT policies and best practices will also need to develop and adapt to counter the new threats.

9. The FATF Recommendations provide the international standard for combating money laundering and terrorist financing and the Recommendations and the criteria set out in this Methodology 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, it is acceptable that countries implement the international standards in a manner consistent with their national legislative and institutional systems, even though the methods by which compliance is achieved may differ. In this regard, assessors should be aware of each country's stage of economic development, its range of administrative capacities, and different cultural and legal conditions. Moreover, the report should provide the context for the assessment, and make note of any progress that has been or is being made in implementing the international standards and the criteria in this Methodology.

#### The Criteria

10. The following set of criteria for each of the FATF Recommendations are listed under two separate headings: "essential criteria" and "additional criteria". The essential criteria are those elements that should be present in order to demonstrate full compliance with a Recommendation. The additional criteria are optional elements that further strengthen the AML/CFT system and may be desirable.

11. The essential criteria are based on the FATF Recommendations, though in a limited number of criteria the wording of the criteria may go beyond the literal wording of the Recommendations e.g. criteria 1.2. The additional criteria are derived from non-mandatory requirements in the FATF Recommendations or on Best Practice and other guidance issued by the FATF, or by the Basel Committee on Banking Supervision. As the essential criteria are the elements that must all be met to comply with the FATF Recommendations, they also provide the basis for any self-assessment exercises.

12. Criteria to be assessed are numbered sequentially for each Recommendation, but the sequence of criteria is not important [– all essential criteria are equally important in determining whether a country is compliant with a Recommendation]. In some cases elaboration (indented below the criteria) is provided in order to assist in identifying important aspects of the assessment of the criteria.

#### Compliance Ratings

13 For each Recommendation there are four possible levels of compliance: compliant, largely compliant, partially compliant, and non-compliant. A country is compliant with a Recommendation whenever the Recommendation is fully observed. A requirement is considered largely compliant when there are only minor shortcomings or a large majority of the essential criteria are fully met, and there are no major concerns. A requirement is considered partially compliant when the country has taken some action and complies with some of the essential criteria, but several essential criteria or key essential criteria are not met. A requirement is considered non-compliant whenever the country has not addressed the issue or has addressed it in a manner that cannot reasonably lead to compliance with any of the essential criteria. A requirement or part of a requirement is considered not applicable whenever, in the view of the assessor, the requirement does not apply, given the structural, legal and institutional features of a country e.g. a particular type of financial institution does not exist in that country.

14. Assessors should review whether the laws and regulations meet the appropriate standard and whether there is adequate capacity and implementation of those laws. Countries should only be regarded as fully complying with criteria if the relevant laws, regulations or other AML/CFT measures are in force and effect at the time of the on-site visit to the country or in the period immediately following the on-site mission, and before the finalisation of the report.

15. Laws 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 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 this Methodology. Assessors should be aware of, and have regard to any assessments or findings made with respect the Core Principles. 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.

## General Interpretation and Guidance

16. Set out below are key definitions from the FATF Recommendations that are used throughout the Methodology[2], and guidance on other points of general interpretation.

**Countries** – all references in the FATF Recommendations and in this Methodology to "countries" apply equally to "territories" or "jurisdictions".

**Designated non-financial businesses and professions (DNFBP)** means:

a) Casinos (which also includes internet casinos).
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 measures that would combat money laundering.
f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust[3];
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

[2] A full set of definitions from the Forty Recommendations and the Eight Special Recommendations are at Annexes 2 & 3.

[3] 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 e.g. constructive trust.

**Financial Institutions**[4] means:

"Any person or entity 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.[i]
2. Lending[ii]
3. Financial leasing.[iii]
4. The transfer of money or value.[iv]
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, CDs, derivatives etc.);
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
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.[v]
13. Money and currency changing.

i. This also captures private banking.
ii. This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).
iii. This does not extend to financial leasing arrangements in relation to consumer products.
iv. This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. 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 Interpretative Note to Special Recommendation VII.
v. This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

**Financing of terrorism** (FT) includes the financing of terrorist acts, and of terrorists and terrorist organisations.

**Should** – For the purposes of assessing compliance with the FATF Recommendations, the word "should" has the same meaning as "must".

**Supervisors** refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

---

[4] As an aide-memoire for assessors, Annex 1 to the Methodology sets out a list of examples of types of financial institutions that engage in the financial activities referred to in the definition.

17. **Requirements for financial institutions and designated non-financial businesses and professions** - The FATF Recommendations state that financial institutions or designated non-financial businesses and professions "should" or "should be required by law or regulation to" take certain actions. These references require countries or their competent authorities to take measures that will oblige their financial institutions or designated non-financial businesses and professions to comply with each of the relevant Recommendations. In the Methodology, in order to use one consistent phrase, the criteria relevant to financial institutions use the phrase "Financial institutions should be required" (a similar approach is taken for designated non-financial businesses). The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation[5] and the criteria that are basic obligations are marked with an asterisk (*). More detailed elements in Recommendations 5, 10 and 13, as well as obligations under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority[6].

18. **Consider** - references in the Recommendations that require a country to "consider" taking particular measures means that the country should have made a proper consideration or assessment of whether to implement such measures, including reaching justified conclusions. Evidence of that assessment should be available to assessors.

19. **Assessment for designated non-financial businesses and professions** - Under Recommendations 12 and 16 designated non-financial businesses and professions should be required to take certain actions. Assessors should assess compliance on the basis that all the designated categories of non-financial businesses and professions should meet the requirements set out in the Recommendation. However, it is not necessary to require these actions through laws, regulations or other 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, regulations or other enforceable means covering the underlying activities. Assessors should note that compliance by designated non-financial businesses and professions with all the necessary AML/CFT measures is to be assessed under Recommendations 12 & 16, and not under other Recommendations.

20. **Risk of money laundering or terrorist financing** - For each Recommendation and each criteria where a financial institution should be required to take certain actions, assessors should normally assess compliance on the basis that all financial institutions should have to meet all the specified requirements. However, a relevant consideration underlying the FATF Recommendations is the degree of risk of money laundering or terrorist financing for particular types of financial institutions or for particular types of customers, products or transactions. A country may therefore take risk[7] into account, and in the circumstances set out below, and subject to the relevant conditions being met, it may decide to limit the application of certain FATF Recommendations (either fully or in part).

21. The circumstances and conditions are:

(a) When a financial activity referred to in the definition of "financial institution" above is carried out on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering or terrorist financing activity occurring. An example might be a hotel providing money exchange facilities to guests, where the limit on the amount that can be exchanged is small.

(b) In other circumstances where there is a proven low risk of money laundering and terrorist financing, a country may decide not to apply some or all of the requirements in one or more Recommendations. However, this should only be done on a strictly limited and justified basis.

---

[5] **Law or regulation** refers to primary and secondary legislation, such as laws, decrees, regulations, or other similar requirements, usually issued under the authority of a legislative body, and which impose mandatory requirements.

[6] **Other enforceable means** refers to guidelines or other documents or mechanisms (other than laws or regulations) that set out enforceable requirements for which there are sanctions for non-compliance (see R.17), and which are issued by a competent authority or appropriately authorised person or body.

[7] All references to "risk" in this Methodology refer to the risk of money laundering and/or terrorist financing.

For the purposes of this Methodology, assessors should be satisfied as to the adequacy of the process to determine low risk and the reasonableness of the conclusions.

22. In Recommendation 5 there are a number of criteria which allow countries to permit their financial institutions to take risk into account when determining the extent of the customer due diligence measures that the institution must take. This should not allow financial institutions to completely avoid doing the required measures, but could allow them to reduce or simplify the measures they have to take for certain criteria. Assessors need to be satisfied that there is an adequate mechanism by which competent authorities assess or review the procedures adopted by financial institutions to determine the degree of risk and how they manage that risk, as well as to review the determinations made by institutions.

23. In Recommendations 5 and 9, reference is made to a financial institution being satisfied as to a matter. This also requires that the institution must be able to justify its assessment to competent authorities, and that assessors need to be satisfied that there is an adequate mechanism by which competent authorities can review the assessments of financial institutions.

24. **Use of examples** – in a number of Recommendations, for particular criteria, examples are provided of situations in which a particular requirement should apply, or where there may be exceptions to the normally applicable obligations. The examples are not part of the criteria, and are only illustrative. However, assessors should use them as guidance as to whether national measures for particular criteria may be appropriate.

25. **Effective implementation** – it is essential that all the FATF Recommendations are effectively implemented, and that assessments or evaluations address this. For some Recommendations this may only require, for example, that the necessary law or regulation has been enacted and is in force, while for others it may require both the law as well as other implementing measures. In certain Recommendations specific types of implementation measures or processes that must be taken are mentioned.

# THE FORTY RECOMMENDATIONS - CRITERIA

## A. LEGAL SYSTEMS

*Scope of the Criminal Offence of Money Laundering*

**Recommendation 1**

The criteria listed below should be read in conjunction with the text of Recommendation 1, Special Recommendation II, and the definition of "designated categories of offences" in the Glossary. (Note to assessors: Ensure that the assessments of Criteria 1.3 – 1.6 and Criteria II.2 – II.3 (in SR.II) are consistent.)

**Essential criteria**

1.1 Money laundering should be criminalised on the basis of the 1988 UN Convention Against Illicit Traffic in Narcotic Drugs and Pyschotropic Substances (the Vienna Convention) and the 2000 UN Convention Against Transnational Organized Crime (the Palermo Convention) i.e. the physical and material elements of the offence (see Article 3(1)(b)&(c) Vienna Convention and Article 6(1) Palermo Convention).

1.2 The offence of ML 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.

1.3 The predicate offences for money laundering should cover all serious offences, and countries should seek to extend this to 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. Where the designated category is limited to a specific offence, then that offence must be covered.

1.4 Where countries apply a threshold approach or a combined approach that includes a threshold approach[8], predicate offences should at a minimum comprise all offences:

a) that fall within the category of serious offences under their national law; or
b) which are punishable by a maximum penalty of more than one year's imprisonment; or
c) which 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).

Examples of categories of serious offences include: "indictable offences" (as opposed to summary offences), "felonies" (as opposed to misdemeanours); "crimes" (as opposed to délits).

1.5 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.

1.6 The offence of money laundering should apply to persons who commit the predicate offence. However, 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.

[8] Countries determine the underlying predicate offences for money laundering 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.

1.7 There should be appropriate ancillary offences to the offence of money laundering[9], including conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

**Additional criteria**

1.8 Countries may provide that it is a money laundering offence in circumstances where the proceeds of crime are derived from conduct that occurred in another country, which is not an offence in that other country but which would have constituted a predicate offence had it occurred domestically.

[9] Subsequent references in this Methodology to a money laundering (ML) offence refer not only to the primary offence or offences, but also to ancillary offences.

## Recommendation 2

The criteria listed below should be read in conjunction with the text of Recommendation 2.

### Essential criteria

2.1 The offence of ML should apply at least to natural persons that knowingly engage in ML activity.

2.2 The law should permit the intentional element of the offence of ML to be inferred from objective factual circumstances.

2.3 The offence of ML should extend to legal persons (e.g., companies, foundations), and, where that is not possible, civil or administrative liability should apply.

*[DG to add examples of "where that is not possible"]*

2.4 Making legal persons subject to criminal liability for ML should not preclude the possibility of parallel criminal, civil or administrative proceedings in countries in which more than one form of liability is available.

2.5 Natural and legal persons should be subject to effective, proportionate and dissuasive criminal, civil or administrative sanctions for ML.

*Provisional Measures and Confiscation*

**Recommendation 3**

The criteria listed below should be read in conjunction with the text of Recommendation 3 and Special Recommendation III. (Note to assessors: Ensure that the assessments of Criteria 3.1 – 3.4, Criterion 3.6 and Criterion III.11 (in SR.III) are consistent.)

**Essential criteria**

3.1 Laws should provide for the confiscation of property[10] that has been or is:

a) laundered;
b) proceeds from;
c) instrumentalities used in; and
d) instrumentalities intended for use in

the commission of any ML, FT or other predicate offences, and property of corresponding value (referred to as "property subject to confiscation").

3.1.1 Criteria 3.1 should equally apply to property that is derived directly or indirectly from proceeds of crime; including income, profits or other benefits from the proceeds of crime.

3.2 Laws and other measures should provide for provisional measures, including the freezing and/or seizing of property, to prevent any dealing, transfer or disposal of property that is or may become subject to confiscation.

3.3 Laws or 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.

3.4 Law enforcement agencies, the FIU or other competent authorities should be given adequate powers to identify and trace property that is, or may become subject to confiscation or is suspected of being the proceeds of crime.

3.5 Laws and other measures should provide protection for the rights of bona fide third parties. Such protection should be consistent with the standards provided in the Palermo Convention.
*[DG to review]*

3.6 There should be authority to take steps to prevent or void actions, whether contractual or otherwise, where the persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in their ability to recover property subject to confiscation.

**Additional criteria**

3.7 Countries may consider laws that provide for the confiscation of:

a) The property of organisations that are found to be primarily criminal in nature (i.e. organisations whose principal function is to perform or assist in the performance of illegal activities).

[10] 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.

b) Property subject to confiscation, but without a conviction of any person (*civil forfeiture*), in addition to the system of confiscation triggered by a criminal conviction.

c) Property subject to confiscation, and which require an offender to demonstrate the lawful origin of the property

## B. MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NON-FINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

### Recommendation 4

The criteria listed below should be read in conjunction with the text of Recommendation 4.

### Essential criteria

4.1 Countries should ensure that no financial institution secrecy law will inhibit the implementation of the FATF Recommendations. 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 R.7, R.9 or SR.VII.

***Customer Due Diligence and Record-keeping***

## Recommendation 5

The criteria listed below should be read in conjunction with the text of Recommendations 5 and 8, Special Recommendation VII, the Interpretative Notes to Recommendation 5, 12 and 16, and to Recommendation 5, and the definitions of "beneficial owner", "designated threshold", "legal arrangements" and "legal persons" in the Glossary. (Note to assessors: Ensure that the assessments of Criteria 5.2 – 5.3 and Criterion VII.1 (in SR.VII) are consistent.)

### Essential criteria

5.1* Financial institutions should not be permitted to keep anonymous accounts[11] or accounts in fictitious names.

*Note to assessors [add reference to wire transfers]*

Where numbered accounts exist, financial institutions should be required to maintain them in such a way that full compliance can be achieved with the FATF Recommendations. For example, the financial institution should properly identify the customer in accordance with these criteria, and the customer identification records should be available to the AML/CFT compliance officer, other appropriate staff and competent authorities.

*When CDD is required*[12]

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

a) establishing business relations;
b) carrying out occasional transactions above the applicable designated threshold (USD/€ 15,000). This also includes situations where the transaction is carried out in a single operation or in several operations [if factual indications exist that there is a connection between those operations] [that appear to be linked];
c) carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII;
d) there is a suspicion of money laundering or terrorist financing, 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*[13]

5.3* Financial institutions should be required to identify the customer (whether permanent or occasional) and verify that customer's identity using reliable, independent source documents, data or information[14].

---

[11] The reference to "accounts" should be read as including other similar business relationships between financial institutions and their customers.

[12] Financial institutions do not have to repeatedly perform identification and verification every time that a customer conducts a transaction.

[13] The general rule is that customers should be subject to the full range of CDD measures. However, there are circumstances in which it would be reasonable for a country to allow its financial institutions to apply the extent of the CDD measures on a risk sensitive basis.

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

5.3.1[*] For customers that are natural persons, the financial institution should be required to obtain sufficient identification data to be satisfied[15] as to the identity of the customer[16].

5.3.2[*] For customers that are legal persons or legal arrangements, the financial institution should be required to:

(a) verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person; and
(b) verify the legal status of the legal person or legal arrangement, e.g. by obtaining proof of incorporation or similar evidence, and obtain information concerning the customer's name, the names of trustees, *[DG to review]* legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement.

5.4* Financial institutions should be required to identify the beneficial owner[17], and take 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.

5.4.1* For all customers, the financial institution should determine whether the customer is acting on behalf of another person, and should then take reasonable steps to obtain sufficient identification data to verify the identity of that other person[18].

5.4.2[*] For customers that are legal persons or legal arrangements, the financial institution should be required to:

(a) take reasonable measures to understand the ownership and control structure of the customer;
(b) determine who are the natural persons that ultimately own or control the customer. This includes those persons who exercise ultimate effective control over a legal person or arrangement.

Examples of the types of measures that would be normally needed to satisfactorily perform this function include:

- For companies - identifying the natural persons with a controlling interest and the natural persons who comprise the mind and management of company.
- For trusts - identifying the settlor, the trustee or person exercising effective control over the trust, and the beneficiaries.

Relevant information or data should be obtained from a reliable source, which could be a public register, the customer or other reliable sources.

Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements i.e. a public company listed on a recognised stock exchange, it is not necessary to seek to identify and verify the identity of the [controlling] shareholders of that company as such information should be publicly available.

---

[15] 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.

[16] Examples of the types of customer information that could be obtained, and the identification data that could be used to verify that information is set out in the paper entitled General Guide to Account Opening and Customer Identification issued by the Basel Committee's Working Group on Cross Border Banking.

[17] "Beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

[18] Financial institutions engaged in insurance business, as set out under item 12 in the definition, must identify and verify the identity of the policy holder (the customer) and the beneficiary under the insurance contract (where that person is different to the policy holder).

5.5 Financial institutions should be required to obtain information on the purpose and intended nature of the business relationship.

5.6* Financial institutions should be required to conduct ongoing due diligence on the business relationship.

5.6.1 Ongoing due diligence should include 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, and where necessary, the source of funds.

5.6.2 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 regular reviews of existing records, particularly for higher risk categories of customers or business relationships.

5.7 Where financial institutions are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by the competent authorities.

*Risk*

5.8 Financial institutions should be required to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction.

Examples of higher risk categories (which are derived from the Basle CDD Paper) may include:

a) Non-resident customers,
b) Private banking,
c) Legal persons or arrangements[such as trusts,] that are personal assets holding vehicles,
d) Companies that have nominee shareholders or shares in bearer form.

Types of enhanced due diligence measures may include those set out in Recommendation 6.

5.9 Countries may permit financial institutions to take reduced or simplified CDD measures only when the risk of money laundering or terrorist financing has been determined to be lower. The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

Examples of customers, transactions or products where the risk may be lower[19] could include:

a) Financial institutions – provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those requirements.
b) Public companies that are subject to regulatory disclosure requirements. This refers to companies that are listed on a stock exchange or similar situations.
c) Government administrations or enterprises.
d) Life insurance policies where the annual premium is no more than USD/€1000 or a single premium of no more than USD/€2500.

[19] Assessors should determine in each case whether the risks are lower having regard to the type of customer, product or transaction, or the location of the customer.

e) Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.

f) 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.

g) Beneficial owners of pooled accounts held by DNFBP provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring compliance with those requirements.

5.10 Where financial institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, the competent authority should limit this to countries that it has determined are in compliance with and have effectively implemented the FATF Recommendations. *[DG to review with respect to IN.13]*

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

*Timing of verification*

5.12 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.

5.13 Countries may permit financial institutions to complete the verification of the identity of the customer and beneficial owner following 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.

Examples of situations where it may be permitted are:

- 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.
- Life insurance business – in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

(c) The money laundering risks are effectively managed.

Where a customer is permitted to utilise the business relationship prior to verification, financial institutions should be required to adopt risk management procedures concerning the conditions under which this may occur. 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 of expected norms for that type of relationship.

*Failure to satisfactorily complete CDD*

5.14 Where the financial institution is unable to comply with Criteria 5.3. to 5.5. above, it should:

a) not be permitted to open the account, to commence business relations and to perform the transaction; and
b) consider making a suspicious transaction report.

5.15 Where the financial institution has already commenced the business relationship e.g. when Criteria 5.2(e), 5.13 or 5.16 apply, and the financial institution is unable to comply with Criteria 5.3 to 5.5 above it should be required to terminate the business relationship.

*Existing customers*

5.16 Financial institutions should be required to apply CDD requirements to existing customers[20] on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times.

For financial institutions engaged in banking business (and for other financial institutions where relevant) - examples of when it may otherwise be an appropriate time to do so is when: (a) a transaction of significance takes place, (b) customer documentation standards change substantially, (c) there is a material change in the way that the account is operated, (d) the institution becomes aware that it lacks sufficient information about an existing customer.

5.17 Financial institutions should be required to perform CDD measures on existing customers if they are customers to whom Criteria 5.1 applies.

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

## Recommendation 6

The criteria listed below should be read in conjunction with the text of Recommendation 6, its Interpretative Note, and the definition of "politically exposed persons" (PEPS) in the Glossary.

### Essential criteria

6.1 Financial institutions should be required, in addition to performing the CDD measures required under R.5, to put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person.

Examples of measures that could form part of such a risk management system include seeking relevant information from the customer, referring to publicly available information or having access to commercial electronic databases of PEPS.

6.2 Financial institutions should be required to obtain senior management approval for establishing business relationships with a PEP.

6.2.1 Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, financial institutions should be required to obtain senior management approval to continue the business relationship.

6.3. Financial institutions should be required to take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPS.

6.4. Where financial institutions are in a business relationship with a PEP, they should be required to conduct enhanced ongoing monitoring on that relationship.

### Additional criteria

6.5 Countries should consider extending the requirements of R.6 to PEPS who hold prominent public functions in their own country. (Note: the Interpretative Note encourages countries to do this)

## Recommendation 7

The criteria listed below should be read in conjunction with the text of Recommendation 7 and the definition of "payable-through accounts" in the Glossary.

### Essential criteria

In relation to cross-border correspondent banking[21] and other similar relationships[22] financial institutions should, in addition to performing any CDD measures that may be required under R.5, be required to take the measures set out in Criteria 7.1-7.5.

7.1 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.

7.2 Assess the respondent institution's AML/CFT controls, and ascertain that they are adequate and effective.

7.3 Obtain approval from senior management before establishing new correspondent relationships.

7.4 Document[23] the respective AML/CFT responsibilities of each institution.

7.5 Where a correspondent relationship involves the maintenance of "payable-through accounts", financial institutions should be satisfied that:

(a) their customer (the respondent financial institution) has performed all the normal CDD obligations set out in R.5 on those of its customers that have direct access to the accounts of the correspondent financial institution; and
(b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

---

[21] 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 of funds, cheque clearing, payable-through accounts and foreign exchange services.

[22] [Similar relationships to which financial institutions should apply Criteria 7.1-7.5 include those established for securities transactions, funds transfers, or other financial transactions, whether for the cross-border financial institution as principal or for its customers].

[23] [It is not necessary that the two financial institutions always have to reduce the respective responsibilities into a written form provided there is a clear understanding as to which institution will perform the required measures]

## Recommendation 8

The criteria listed below should be read in conjunction with the text of Recommendation 8.

### Essential criteria

8.1 Financial institutions should be required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.

8.2 Financial institutions should be required to have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. These policies and procedures should apply when establishing customer relationships and when conducting ongoing due diligence.

Examples of non-face to face operations include: business relationships concluded over the Internet or by other means such as through the post, services and transactions over the Internet including trading in securities by retail investors over the Internet or other interactive computer services, use of ATM machines, telephone banking, transmission of instructions or applications via facsimile or similar means and making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or reloadable or account-linked value cards.

8.2.1 Measures for managing the risks should include specific and effective CDD procedures that apply to non-face to face customers.

Examples of such procedures include: the certification of documents presented; the requisition of additional documents to complement those which are required for face-to-face customers; develop independent contact with the customer; rely on third party introduction (see criteria 9.1 to 9.5) and require the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

Financial institutions should refer to the CDD Paper, Section 2.2.6.

For electronic services, financial institutions could refer to the "Risk Management Principles for Electronic Banking" issued by the Basel Committee in July 2003.

## Recommendation 9

The criteria listed below should be read in conjunction with the text of Recommendation 9 and its Interpretative Note.

Note: This Recommendation does not apply to:

(a) outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the financial institution to carry out its CDD functions[24];
(b) business relationships, accounts or transactions between financial institutions for their clients which are addressed by R.5 and R.7. *[DG to review reference to R.5]*

## Essential criteria

If financial institutions are permitted to rely on intermediaries or other third parties[25] to perform some of the elements of the CDD process (Criteria 5.3 to 5.5)[26] or to introduce business, then the following criteria should be met.

9.1 Financial institutions relying upon a third party should be required to immediately obtain from the third party the necessary information[27] concerning certain elements of the CDD process (Criteria 5.3 to 5.5).

9.2 Financial institutions should be required to take adequate steps to satisfy themselves 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.

9.3 Financial institutions should be required to satisfy themselves that the third party is regulated and supervised [or monitored] for (in accordance with Recommendations 23 or 24), and has measures in place to comply with, the CDD requirements set out in R.5 and R.10.

9.4 In determining in which countries the third party that meets the conditions can be based, competent authorities should take into account information available on whether those countries adequately apply the FATF Recommendations[28].

9.5 The ultimate responsibility for customer identification and verification should remain with the financial institution relying on the third party.

---

[24] Where there is a contract to outsource CDD, R.9 does not apply because the outsource or agent is to be regarded as synonymous with the financial institution i.e. the processes and documentation are those of the financial institution itself

[25] Intermediaries or other third parties can be financial institutions, DNFBP or other reliable persons or businesses that meet Criteria 9.1 to 9.4.

[26] In practice, this reliance on third parties often occurs through introductions made by another member of the same financial services group, or in some jurisdictions from another financial institution or third party. It may also occur in business relationships between insurance companies and insurance brokers/agents, or between mortgage providers and brokers.

[27] It is not necessary to obtain copies of documentation.

[28] Countries should refer to reports, assessments or reviews concerning AML/CFT that are published by the FATF, FSRBs, the IMF or World Bank.

**Recommendation 10**

The criteria listed below should be read in conjunction with the text of Recommendation 10 and its Interpretative Note.

**Essential criteria**

10.1* Financial institutions should be required to maintain all necessary records on transactions[29], both domestic and international, for at least five years following completion of the transaction (or longer if requested by a competent authority in specific cases and upon proper authority). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated.

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

Examples of the necessary components of transaction records include: customer's (and beneficiary's) name, address (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction.

10.2* Financial institutions should be required to maintain records of the identification data, account files and business correspondence for at least five years following the termination of an account or business relationship (or longer if requested by a competent authority in specific cases upon proper authority).

10.3* Financial institutions should be required to ensure that all customer and transaction records and information are available on a timely basis to domestic competent authorities upon appropriate authority.

[29] In the insurance sector, the word « transactions » should be understood to refer to the insurance product itself, the premium payment and the benefits. For specific requirements with regard to record keeping of transactions in the insurance sector, see the IAIS Guidance Notes of January 2002.

## Recommendation 11

The criteria listed below should be read in conjunction with the text of Recommendation 11 and its Interpretative Note.

### Essential criteria

11.1 Financial institutions should be required to pay special attention to all complex, unusual large transactions[30], or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose.

Examples of such transactions or patterns of transactions include: significant transactions relative to a relationship, transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance, or transactions which fall out of the regular pattern of the account's activity.

11.2 Financial institutions should be required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing.

11.3 Financial institutions should be required to keep such findings available for competent authorities and auditors for at least five years.

[30] In the insurance sector, the word « transactions » should be understood to refer to the insurance product itself, the premium payment and the benefits.

**Recommendation 12**

The criteria listed below should be read in conjunction with the text of Recommendation 12, the Interpretative Note to R.5, 12 & 16, and the Criteria for Recommendations 5, 6 and 8-11.

**Essential criteria**

12.1 DNFBP should be required to comply with the requirements set out in Recommendation 5 (Criteria 5.1 – 5.17) in the following circumstances[31]:

a) Casinos (including internet casinos) – when their customers engage in financial transactions equal to or above USD/€ 3,000[32].

Examples of such financial transactions include: the purchase of casinos chips or tokens, the opening of accounts, wire transfers and currency exchanges.

b) Real estate agents – when they are involved in transactions for a 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 USD/€ 15,000[32].

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for a client in relation to the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets[33];
- management of bank, savings or securities accounts[33];
- 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 and when they carry out transactions for a client in relation to 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;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

[31] The designated thresholds applied in these criteria are referred to in the IN of R. 5, 12 and 16

[32] The designated thresholds of USD/€ 3,000 and USD/€ 15,000 include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

[33] Where the lawyer, notary, other independent legal professional or accountant is conducting financial activity as a business and meets the definition of "financial institution" then that person or firm should comply with the requirements applicable to financial institutions.

DNFBP should especially comply with the CDD measures set out in Criteria 5.3 to 5.6 but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction.

12.2 In the circumstances set out in Criteria 12.1, DNFBP should be required to comply with the criteria set out under Recommendations 6 and 8-11.

*[DG to review in line with issues raised by the Secretariat. Issue of sanctions]*

*Reporting of Suspicious Transactions and Compliance*

## Recommendation 13

The criteria listed below should be read in conjunction with the text of Recommendation 1, Recommendation 13 and its Interpretative Note, and the text of Special Recommendation IV. (Note to assessors: Ensure that the assessments of Criteria 13.1 – 13.4 and Criteria IV.1 – IV.2 (in SR.IV) are consistent.)

### Essential criteria

13.1* A financial institution should be required by law or regulation to report to the FIU (a suspicious transaction report – STR) when it suspects or has reasonable grounds to suspect[34] that funds[35] are the proceeds[36] of a criminal activity. At a minimum, the obligation to make a STR should apply to funds that are the proceeds of all offences that are required to be included as predicate offences under Recommendation 1. This 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 ML offence or otherwise (so called "indirect reporting"), is not acceptable.

13.2* The obligation to make a STR also applies to funds where there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism.

13.3* All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

13.4* The requirement to report suspicious transactions should apply regardless of whether they are thought, among other things, to involve tax matters.

### Additional criteria

13.5. Countries should consider requiring financial institutions to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction. (Note: the Interpretative Note strongly encourages countries to do this).

---

[34] The requirement to report when the individual "suspects" is a subjective test of suspicion i.e. the person actually suspected that a transaction involved a criminal activity. A requirement to report when there are "reasonable grounds to suspect" is an objective test of suspicion and can be satisfied if the circumstances surrounding the transaction would lead a reasonable person to suspect that the transaction involved a criminal activity. This requirement implies that countries may choose either the two alternatives, but need not have both.

[35] *Funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable and legal documents or instruments evidencing title to, or interest in, such assets.

[36] *Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.

## Recommendation 14

The criteria listed below should be read in conjunction with the text of Recommendation 14 and its Interpretative Note.

### Essential criteria

14.1. Financial institutions and their directors, officers and employees (permanent and temporary) 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.

14.2. Financial institutions and their directors, officers and employees (permanent and temporary) should be prohibited by law from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU.

### Additional criteria

14.3. Countries should consider enacting laws or regulations or taking other measures, consistent with the principles of domestic laws that will ensure that the names and personal details of staff of financial institutions that make a STR are kept confidential by the FIU.

**Recommendation 15**

The criteria listed below should be read in conjunction with the text of Recommendation 15, its Interpretative Note, and the definitions of "legal arrangements" and "legal persons" in the Glossary.

**Essential criteria**

The type and extent of measures to be taken for each of the requirements set out below should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

15.1 Financial institutions should be required to establish and maintain internal procedures, policies and controls to prevent ML and FT, and to communicate these to their employees. These procedures, policies and controls should cover, *inter alia,* CDD, record retention, the detection of unusual and suspicious transactions and the reporting obligation, [and should extend to foreign branches and majority owned subsidiaries. ]

15.1.1 Financial institutions should be required to develop appropriate compliance management arrangements e.g. for financial institutions at a minimum the designation of an AML/CFT compliance officer at the management level.

15.1.2 The AML/CFT compliance officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

15.2 Financial institutions should be required to maintain an adequately resourced and independent audit function to test compliance (including sample testing) with these procedures, policies and controls.

15.3 Financial institutions should be required to establish ongoing employee training to ensure that employees are kept informed of new developments, including information on current ML and FT techniques, methods and trends; and that there is a clear explanation of all aspects of AML/CFT laws and obligations, and in particular, requirements concerning CDD and suspicious transaction reporting.

15.4. Financial institutions should be required to put in place screening procedures to ensure high standards when hiring employees.

**Additional criteria**

15.5. The AML/CFT compliance officer at the management level should able to act independently and to report to the board of directors.

## Recommendation 16

The criteria listed below should be read in conjunction with the text of Recommendation 16 and its Interpretative Note, Recommendations 13-15 and their Interpretative Notes and criteria, Special Recommendation IV, and the definitions of "designated non-financial businesses and professions", "designated threshold", "FIU" and "STR". (Note to assessors: Ensure that the assessments of Criteria 16.1 – 16.3 and Criteria IV.1 – IV.3 (in SR.IV) are consistent.)

### Essential criteria

16.1 DNFBP should be required to comply with the requirements set out in Recommendation 13 (Criteria 13.1 – 13.4)[37] in the following circumstances:

a) Casinos (which includes internet casinos) – any transaction (as for financial institutions).
b) Real estate agents - any transaction (as for financial institutions).
c) Dealers in precious metals or stones - when they engage in any cash transaction equal to or above USD/€ 15,000[38].
d) Lawyers, notaries, other independent legal professionals and accountants - when, on behalf of or for a client, they engage in a financial transaction in relation to 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.

**Note on professional secrecy or legal professional privilege.**

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 jurisdiction 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. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

e) Trust and Company Service Providers - when they prepare for or carry out a transaction on behalf of a client, in relation to the following activities:

- acting as a formation agent of legal persons;

---

[37] DNFBP should comply with all the criteria in Recommendation 13 with two exceptions. First, dealers in precious metals and stones must comply with criteria 13.3, but would only be required to report transactions (or attempted transactions) above the cash threshold of USD/€ 15,000. Second, as detailed in criteria 16.1, countries may allow lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals to send their STR to self-regulatory organizations, and they do not always need to send STR to the FIU.

[38] The designated threshold includes situations where the transaction is carried out in a single operation or in several operations that appear to be linked (cases of "smurfing"/"structuring").

- 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;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

16.2 Where countries allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations[39] (SRO), there should be appropriate forms of co-operation between these organisations and the FIU. Each country should determine the details of how the SRO could co-operate with the FIU.

16.3 In the circumstances set out in criteria 16.1, the criteria set out under Recommendations 14, 15 and 21 should apply in relation to DNFBP.

**Additional criteria**

16.4. Countries should consider extending the reporting requirement to the rest of the professional activities of accountants, including auditing.

[16.5 Countries to consider extending the requirements in criteria 13.5 to DNFBP]

*DG to examine issue of sanctions R.17]*

[39] A SRO is a body that represents the profession, and which is made up of member professionals, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory type functions. For example, it would be normal for this body to enforce rules to ensure that high ethical and moral standards are maintained by those practicing the profession.

***Other Measures to Deter Money Laundering and Terrorist Financing***

## Recommendation 17

The criteria listed below should be read in conjunction with the text of Recommendation 17, Special Recommendations IV, VI and VII, and the definition of "legal persons" in the Glossary. (Note to assessors: Ensure that Criteria 17.1 – 17.4 and Criterion IV.4 (in SR.IV), Criterion VI.5 (in SR.VI) and Criterion VII.9 (in SR.VII) are consistent.)

### Essential criteria

17.1 Countries should ensure that effective, proportionate and dissuasive criminal, civil or administrative sanctions are available to deal with natural or legal persons covered by the FATF Recommendations that fail to comply with national AML/CFT requirements.

17.2 Countries should designate an authority (e.g. supervisors, the self-regulatory organisations referred to in Recommendation 24 or the FIU) empowered to apply these sanctions. Different authorities may be responsible for applying sanctions depending on the nature of the requirement that was not complied with.

17.3 Sanctions should be available in relation not only to the legal persons that are financial institutions or businesses but also to their directors and senior management.

17.4 The range of sanctions available should be broad and proportionate to the severity of a situation. At a minimum, they should include the power to impose disciplinary and financial sanctions and the power to withdraw, restrict or suspend the financial institution's license, where applicable. [Relevant sanctions should be available for DNFBP].

> Examples of types of sanctions include: written warnings (separate letter or within an audit report), orders to comply with specific instructions (possibly accompanied with daily fines for non-compliance), criminal proceeding where permitted, 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, or controlling owners, imposing conservatorship or a suspension or withdrawal of the license.

17.5 If a natural or legal person offers financial services or operates as a casino, having failed to obtain any necessary license or registration required under national laws or regulations, that person should be subject to administrative, civil or criminal sanctions. This criterion does not require countries to create licensing or registration systems other than those required under R.24.

*[DG to review references to DNFBP in relation to other Recommendations]*

**Recommendation 18**

The criteria listed below should be read in conjunction with the text of Recommendation 18 and the definition of "shell banks" in the Glossary.

**Essential criteria**

18.1 Countries should not approve the establishment or accept the continued operation of shell banks[40].

18.2 Financial institutions should not be permitted to enter into, or continue, correspondent banking relationships with shell banks.

18.3 Financial institutions should be required to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

[40] Shell bank is defined in the Annex 2. The meaning of physical presence is not defined in these Recommendations. In its paper entitled *Shell banks and booking offices* (July 2002), the Basel Committee defines "physical presence" to be meaningful mind and management and countries should have regard to this paper.

## Recommendation 19

The criteria listed below should be read in conjunction with the text of Recommendation 19 and its Interpretative Note.

### Essential criteria

19.1 Countries should consider implementing measures to detect, monitor or report the cross-border transportation of currency and bearer negotiable instruments.

19.2 Countries should consider implementing a system to report all transactions in currency above a fixed threshold.

### Additional criteria

19.3 Where countries implement systems for reporting cross border or large currency transactions, those reports should be maintained in a computerised data base, available to competent authorities for AML/CFT purposes.

19.4 Any systems for reporting cross border or large currency transactions should be subject to strict safeguards to ensure proper use of the information or data that is reported or recorded.

19.5 Any systems for reporting cross border transactions should not impede in any way the freedom of capital movements.

19.6 If a country discovers an unusual international shipment of currency, monetary instruments, precious metals, or gems, etc., it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which the shipment originated and/or to which it is destined, and should co-operate with a view toward establishing the source, destination, and purpose of such shipment and toward the taking of appropriate action.

## Recommendation 20

The criteria listed below should be read in conjunction with the text of Recommendation 20.

### Essential criteria

20.1 Countries should consider applying Recommendations 5, 6, 8-11, 13-15, 17 and 21 to non-financial businesses and professions (other than DNFBP) that are at risk of being misused for money laundering or terrorist financing.

> Examples of businesses or professions that may be at risk include: dealers in high value and luxury goods, pawnshops, gambling, auction houses, [tax] and investment advisers.

20.2 Countries should take measures to encourage the development and use of modern and secure techniques for conducting financial transactions that are less vulnerable to money laundering.

> Examples of techniques or measures that may be less vulnerable include:
>
> - Not issuing very large denomination banknotes;
> - Ensuring that an audit trail exists for all financial transactions.

## Recommendation 21

The criteria listed below should be read in conjunction with the text of Recommendation 21.

### Essential criteria

21.1 Financial institutions should be required to give special attention to business relationships and transactions with persons (including legal entities and other financial institutions) from or in countries that do not have adequate systems in place to prevent or deter ML or FT, in line with the FATF Recommendations.

21.1.1 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.

21.2 If those transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined, and written findings should be available to assist competent authorities (e.g. supervisors, law enforcement agencies and the FIU) and auditors.

21.3 Where a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate counter-measures.

Examples of possible counter-measures include:

- Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries;
- Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;
- In considering requests for approving the establishment in FATF member countries of subsidiaries or branches or representative offices of financial institutions, taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems;
- Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of money laundering.
- Limiting business relationships or financial transactions with the identified country or persons in that country.

**Recommendation 22**

The criteria listed below should be read in conjunction with the text of Recommendation 22.

**Essential criteria**

*[DG to review]*

22.1 Financial institutions should be required to ensure that their foreign branches and subsidiaries[41] observe AML/CFT measures consistent with home country requirements and the FATF Recommendations, to the extent that local laws and regulations permit.

22.1.1 Financial institutions should be required to pay particular attention that this principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply the FATF Recommendations.

22.2 Where the minimum AML/CFT requirements of the home and host jurisdictions differ, branches and subsidiaries in host jurisdictions should be required to apply the higher standard, to the extent that local laws and regulations permit.

22.3 Financial institutions should be required to inform their home jurisdiction supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local laws, regulations or other measures.

[41] Subsidiaries refers to majority owned subsidiaries

## Recommendation 23

The criteria listed below should be read in conjunction with the text of Recommendation 23, its Interpretative Note, the text of Special Recommendation VI, its Interpretative Note and the definition of "Core Principles".

### Essential criteria

23.1 Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations.

23.2 Countries should ensure that a designated competent authority or authorities has/have responsibility for ensuring that financial institutions adequately comply with the requirements to combat money laundering and terrorist financing.

23.3 Supervisors or other 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, including in the executive or supervisory boards, councils, etc in a financial institution.

23.3.1 Directors and senior management of financial institutions subject to the Core Principles should be evaluated on the basis of "fit and proper" criteria including those relating to expertise and integrity.

23.4 For financial institutions that are subject to the Core Principles[42] the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes, except where specific criteria address the same issue in this Methodology.

> Examples of regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, include requirements for: (i) licensing and structure; (ii) risk management processes to identify, measure, monitor and control material risks; (iii) ongoing supervision (e.g. supervisors should have regular contact with bank management and a thorough understanding of the institution's operations) and (iv) cross-border activities (supervisors should practice global consolidated supervision over internationally-active institutions).

23.5 Businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered.

23.6 Businesses providing a service of money or value transfer, or of money or currency changing should be subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

23.7 Financial institutions (other than those mentioned in Criteria 23.4) should be licensed or registered and appropriately regulated, and subject to supervision or oversight for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector i.e. if there is a proven low risk then the required measures may be less.

*[DG ensure consistency with SRVI]*

---

[42] Note to assessors: Refer to the Core Principles for a precise description of the financial institutions that are covered, but broadly speaking it refers to: (1) banking and other deposit-taking business, (2) insurers and insurance intermediaries, and (3) collective investment schemes and market intermediaries.

**Recommendation 24**

The criteria listed below should be read in conjunction with the text of Recommendation 24.

**Essential criteria**

*[Nexus for internet casinos. Also consider the issue in Rec. 12 & 16]*

24.1 Countries should ensure that casinos (including Internet casinos) are subject to a comprehensive regulatory and supervisory regime and are effectively implementing the AML/CFT measures required under the FATF Recommendations.

24.1.1 Countries should ensure that a designated competent authority has responsibility for the regulatory and supervisory regime.

24.1.2 Casinos should be licensed by a designated competent authority.

24.1.3 A competent authority 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.

24.2 Countries should ensure that the other categories of DNFBP are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining whether the system for monitoring and ensuring compliance is appropriate, regard may be had to the risk of money laundering or terrorist financing in that sector i.e. if there is a proven low risk then the extent of the required measures may be less.

[24.2.1 There should be a designated competent authority or SRO responsible for monitoring and ensuring compliance of DNFBPs with AML/CFT requirements. Such an authority or SRO should:

a) have adequate powers to perform its functions, including powers of inspection and sanction[43];
b) have sufficient technical and other resources to perform its functions[44];
c) be able to co-operate domestically with other competent authorities[45].]

*[DG to review]*

[43] [In assessing compliance with this criterion, assessors should have regard to Criteria 29.1 to 29.5 where it is appropriate to do so (i.e. depending on the type of the designated competent authority or SRO, its size, its responsibilities, etc). ]

[44] In assessing compliance with this criterion, assessors should have regard to Criteria 30.1 to 30.6 where it is appropriate to do so (i.e. depending on the type of the designated competent authority or SRO, its size, its responsibilities, etc).

[45] In assessing compliance with this criterion, assessors should have regard to Criteria 31.1 to 31.3 where this is appropriate (i.e. depending on the type of the designated competent authority or SRO, its size, its responsibilities, etc).

## Recommendation 25

The criteria listed below should be read in conjunction with the text of Recommendation 25 and its Interpretative Note.

### Essential criteria

25.1. Competent authorities should establish guidelines that will assist financial institutions, DNFBP and any other business or profession covered by national measures, to implement and comply with national AML/CFT requirements.

> The guidelines should cover relevant aspects of the national AML/CFT system, and at a minimum should give assistance on issues covered under the relevant FATF Recommendations, including: (i) a description of ML and FT techniques, methods and trends; (ii) an explanation of the AML/CFT laws and requirements that apply; and guidance on how a financial institution, a DNFBP or other business or profession could comply with those laws and requirements; (iii) best practice measures that these institutions, businesses or professions could take to ensure that their AML/CFT measures are effective.

25.2. Competent authorities, and particularly the FIU, should provide financial institutions, DNFBP and any other business or profession that are required to report suspicious transactions, with adequate and appropriate feedback having regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.

> Examples of appropriate feedback mechanisms (drawn from the Best Practices Paper) include:
>
> (i) general feedback - (a) statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures; (b) information on current techniques, methods and trends (typologies); and (c) sanitised examples of actual money laundering cases.
>
> (ii) specific or case by case feedback - (a) acknowledgement of the receipt of the report; (b) if a case is closed or completed, whether because of a concluded prosecution, because the report was found to relate to a legitimate transaction or for other reasons, and if the information is available, then the institution should receive information on that decision or result.

## C. INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

*Competent Authorities, their Powers and Resources*

**Recommendation 26**

The criteria listed below should be read in conjunction with the text of Recommendation 26, its Interpretative Note and the definitions of "FIU" and "STR" in the Glossary.

**Essential criteria**

26.1. Countries should establish an FIU that serves as a national centre for receiving (and if permitted, requesting), analysing, and disseminating disclosures of STR and other relevant information concerning suspected ML or FT activities. The FIU can be established either as an independent governmental authority or within an existing authority or authorities.

26.2 The FIU or another competent authority should provide financial institutions and other reporting parties with guidance regarding the manner of reporting, including the specification of reporting forms, and the procedures that should be followed when reporting.

26.3 The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information and any additional information that it requires to properly undertake its functions, including the analysis of STR.

26.4 The FIU, either directly or through another competent authority, should be authorised to obtain from reporting parties additional information needed to properly undertake its functions.

26.5 The FIU should be authorised to disseminate financial information to domestic authorities for investigation or action when there are grounds to suspect ML or FT.

26.6 The FIU should have sufficient operational independence and autonomy to ensure that it is free from undue outside influence or interference.

26.7 Information held by the FIU should be securely protected and disseminated only in accordance with the law.

26.8 The FIU should publish, including electronically, periodic reports, including statistics, typologies and trends [regarding its activities].
*[DG to review]*

26.9 Where a country has created an FIU, it should consider applying for membership in the Egmont Group.

**Additional criteria**

26.10 Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.

## Recommendation 27

The criteria listed below should be read in conjunction with the text of Recommendation 27, its Interpretative Note and the definitions of "FIU" and "STR" in the Glossary.

### Essential criteria

27.1 There should be designated law enforcement[46] authorities that have responsibility for ensuring that ML and FT offences are properly investigated.

### Additional criteria

27.2 Countries should consider taking measures, whether legislative or otherwise, that will allow their law enforcement or prosecution authorities to have an adequate legal basis for the use of a wide range of special investigative techniques when conducting investigations of ML or FT, such as controlled delivery of the proceeds of crime or funds intended for use in terrorism, undercover operations, etc.

27.3 Where special investigative techniques are permitted, countries should consider developing and supporting the use of such techniques when conducting investigations of ML, FT, and underlying predicate offences. (Note: the Interpretative Note encourages countries to do this)

27.4 Countries should consider using other effective mechanisms such as the use of:

(a) Permanent or temporary groups specialised in investigating the proceeds of crime (financial investigators). An important component of the work of such groups or bodies would be focused on the investigation, seizure, freezing and confiscation of the proceeds of crime.

(b) Co-operative investigations with appropriate competent authorities in other countries, including the use of special investigative techniques, provided that adequate safeguards are in place.

(Note: the Interpretative Note encourages countries to use these mechanisms)

27.5 ML and FT methods, techniques and trends should be reviewed by law enforcement authorities, the FIU and other competent authorities (as appropriate) on a regular, interagency basis, and resulting information, analysis or studies should be disseminated to law enforcement and FIU staff, as well as staff of other competent authorities.

[46] In certain countries, this responsibility also rests with prosecution authorities.

## Recommendation 28

The criteria listed below should be read in conjunction with the text of Recommendation 28.

### Essential criteria

28.1 Competent authorities responsible for conducting investigations of ML, FT and other underlying predicate offences should have the powers to be able to:

a) compel production of,
b) search persons or premises for, and
c) seize and obtain

transaction records, identification data obtained through the CDD process, account files and business correspondence, and other records, documents or information, held or maintained by financial institutions and other businesses or persons. Such powers should be exercised through lawful process (for example, subpoenas, summonses, search and seizure warrants, or court orders) and be available for use in investigations and prosecutions of ML, FT, and other underlying predicate offences, or in related actions e.g. actions to freeze and confiscate the proceeds of crime.

28.2 The competent authorities referred to above should have the powers to be able to take witnesses' statements for use in investigations and prosecutions of ML, FT, and other underlying predicate offences, or in related actions.

## Recommendation 29

The criteria listed below should be read in conjunction with the text of Recommendation 29 and the definition of "supervisors" in the Glossary.

### Essential criteria

29.1 Supervisors should have adequate powers to monitor and ensure compliance by financial institutions, [including their foreign branches and majority-owned subsidiaries,] with requirements to combat money laundering and terrorist financing, consistent with the FATF Recommendations. *[DG to review issue of materiality and prohibition by local laws]*

29.2 Supervisors should [have the authority to] conduct inspections of financial institutions, including on-site inspections, to ensure compliance. Such inspections should include the review of policies, procedures, books and records, and should extend to sample testing. *[DG to review issue of effectiveness]*

29.3 Supervisors should have the power to compel production of or to obtain access to all records, documents or information relevant to monitoring compliance. This includes all documents or information related to accounts or other business relationships, or transactions, including any analysis the financial institution has made to detect unusual or suspicious transactions.

29.3.1 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.

29.4 The supervisor should have adequate powers of enforcement and sanction against financial institutions, and their directors or senior management for failure to comply with or properly implement requirements to combat money laundering and terrorist financing, consistent with the FATF Recommendations, including the power to withdraw or suspend the institution's license (see also R.17)

**Recommendation 30**

The criteria listed below should be read in conjunction with the text of Recommendation 30.

**Essential Criteria**

30.1 FIUs, law enforcement and prosecution agencies, supervisors and other competent authorities involved in combating money laundering and terrorist financing should be adequately structured, funded, staffed, and provided with sufficient technical and other resources to fully and effectively perform their functions. Adequate structuring includes the need for sufficient operational independence and autonomy to ensure freedom from undue outside influence or interference.

30.2 Staff of competent authorities should be required to maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

30.3 Staff of competent authorities should be provided with adequate and relevant training:

a) for combating ML and FT;

Adequate and relevant training should, in particular, concern the scope of predicate offences, ML and FT typologies, techniques to investigate and prosecute these offences, techniques for tracing property that is the proceeds of crime or is to be used to finance terrorism, and ensuring that such property is seized, frozen and confiscated, and the techniques to be used by supervisors to ensure that financial institutions are complying with their obligations.

b) for using information technology and other resources relevant to the execution of their functions.

30.3.1 Countries should provide special training and/or certification for financial investigators for, *inter alia*, investigations of ML, FT, and the predicate offences.

**Additional Criteria**

30.4 Countries should consider providing special training or educational programmes for judges and courts concerning ML and FT offences, and the seizure, freezing and confiscation of property that is the proceeds of crime or is to be used to finance terrorism.

## Recommendation 31

The criteria listed below should be read in conjunction with the text of Recommendation 31.

### Essential Criteria

31.1 Policy makers, the FIU, law enforcement and supervisors and other competent authorities should have effective mechanisms in place which enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

Such mechanisms should normally address:

(a) operational co-operation and, where appropriate, co-ordination between authorities at the law enforcement/FIU level (including customs authorities where appropriate); and between the FIU, law enforcement and supervisors;
(b) policy co-operation and, where appropriate, co-ordination across all relevant competent authorities,.

### Additional Criteria

31.2 Countries should have mechanisms for consultation between competent authorities, the financial sector and other sectors (including DNFBP) that are subject to AML/CFT laws, regulations, guidelines or other measures.

## Recommendation 32

The criteria listed below should be read in conjunction with the text of Recommendation 32.

### Essential Criteria

32.1 Countries should review the effectiveness of their systems for combating money laundering and terrorist financing on a regular basis.

32.2 Competent authorities should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of systems for combating money laundering and terrorist financing. This should include keeping annual statistics on:

(a) suspicious transaction reports (and other reports where appropriate under domestic law) received and disseminated -

- STR received by the FIU, including a breakdown of the type of financial institution, DNFBP, or other business or person making the STR;
- Breakdown of STR analysed and disseminated;
- Reports filed on: (i) domestic or foreign currency transactions above a certain threshold, (ii) cross border transportation of currency and bearer negotiable instruments, [(iii) international wire transfers, or (iv) other transactions related to ML or FT (only where the reporting of such transactions or transportation is required by domestic law).]

(b) ML & FT investigations; prosecutions and convictions, and on property frozen; seized and confiscated -

- ML and FT investigations, prosecutions, and convictions;
- [Any criminal, civil, or administrative sanctions applied to persons convicted of such offences;]
- The number of cases and the amounts of property frozen, seized, and confiscated relating to (i) ML,(ii) FT, and (iii) underlying predicate offences; and
- Number of persons or entities and the amounts of property frozen pursuant to or under U.N. Resolutions relating to terrorist financing.

(c) Mutual legal assistance or other international requests for co-operation -

- All mutual legal assistance and extradition requests (including requests relating to freezing, seizing and confiscation) that are made or received, relating to ML, the predicate offences and FT, including the nature and result of the request, and the time required to respond;
- Other requests for assistance made or received by the FIU, including the result of the request;
- Other requests for assistance made or received by law enforcement authorities relating to ML or FT, including the result of the request; and
- Spontaneous referrals made by the FIU to foreign authorities

(d) Other action

- On-site examinations conducted by supervisors relating to or including AML/CFT and the results of those examinations.
- Requests for assistance made or received by supervisors relating to or including AML/CFT, including the result of the request.

**Additional criteria**

32.3 Competent authorities should consider maintaining comprehensive statistics on STR resulting in investigation, prosecution, or convictions for ML, FT or an underlying predicate offence.

**Recommendation 33**

The criteria listed below should be read in conjunction with the texts of Recommendation 33, and the definitions of "beneficial owner" and "legal persons".

*[Delete footnotes that are in the annex]*

**Essential criteria**

33.1 Countries should take measures to prevent the unlawful use of legal persons[47] in relation to money laundering and terrorist financing by ensuring that their commercial, corporate and other laws require adequate transparency concerning the beneficial ownership and control of legal persons.

*[Ex. Box. DG to review. Check consistency with the OECD Report]*

Examples of mechanisms that countries could use to ensure that there is adequate transparency:

1. A system of central registration where a national registry records the required ownership and control details for all companies and other legal persons registered in that country. The relevant information could be either publicly available or only available to competent authorities. Changes in ownership and control information would need to be kept up to date.

2. Requiring company service providers to obtain, verify and retain records of the beneficial ownership and control of legal persons.

3. Requiring companies and other legal persons to obtain and record the required information, to keep it within the country, and to rely on the investigative and other powers of law enforcement, regulatory or other competent authorities to obtain or have access to the information.

Countries may use a combination of the mechanisms described above.

Whatever mechanism is used it is essential that competent authorities: (a) are able to obtain or have access in a timely fashion to the beneficial ownership and control information, and (b) that the information must be adequate, accurate and timely (see Criterion 33.2).

33.2 Competent authorities should be able to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons.

33.2.1 Competent authorities should be able to share information on the beneficial ownership and control of legal persons with foreign competent authorities (in accordance with the criteria set out in R.36 & 40).

33.3 Countries that have legal persons able to issue bearer shares[48] should take appropriate measures to ensure that they are not misused for money laundering, and that the principles set out in criteria 33.1 and 33.2 above apply equally to legal persons that use bearer shares. The measures to be taken may vary from country to country, but each country should be able to demonstrate the adequacy and effectiveness of the measures that are applied.

Additional criteria

[47] "Legal persons" refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

[48] "Bearer shares" refers to negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate.

33.4 Countries could consider adopting measures to facilitate access by financial institutions to beneficial ownership and control information, so as to allow them to more easily verify the customer identification data.

## Recommendation 34

The criteria listed below should be read in conjunction with the texts of Recommendation 34 and the definitions of "beneficial owner" and "legal arrangements".

*[Delete footnotes that are already in the annex]*

### Essential criteria

34.1 Countries should take measures to prevent the unlawful use of legal arrangements[49] in relation to money laundering and terrorist financing by ensuring that its commercial, trust and other laws require adequate transparency concerning the beneficial ownership and control of trusts and other legal arrangements.

*[Ex. Box. DG to review. Check consistency with the OECD Report]*

Examples of mechanisms that countries could use to ensure that there is adequate transparency:

1. A system of central registration where a national registry records details on trusts (i.e. settlors, trustees, beneficiaries and protectors) and other legal arrangements registered in that country. The relevant information could be either publicly available or only available to competent authorities. Changes in ownership and control information would need to be kept up to date.

2. Requiring trust service providers to obtain, verify and retain records of the details of the trust or other similar legal arrangements.

3. Requiring trustees to obtain, verify and retain records of the required information, to keep it within the country, and to rely on the investigative and other powers of law enforcement, regulatory or other competent authorities to obtain or have access to the information.

Whatever mechanism is used it is essential that competent authorities: (a) are able to obtain or have access in a timely fashion to the beneficial ownership and control information, and (b) that the information must be adequate, accurate and timely (see Criterion 34.2).

34.2 Competent authorities should be able to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal arrangements, and in particular the settlor[50], the trustee[51] and the beneficiaries[52] of express trusts[53].

---

[49] "Legal arrangements" refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.

[50] The settlors are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.

[51] The trustees, who may be paid professionals or companies or unpaid persons, hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes. There may also be a protector, who may have power to veto the trustees' proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.

[52] All trusts (other than charitable or statutory permitted non-charitable trusts) must have beneficiaries, who may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.

53 "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. Express trusts 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.

34.2.1 Competent authorities should be able to share information on the beneficial ownership and control of legal arrangements with foreign competent authorities in accordance with the criteria set out in R.36 & 40.

**Additional criteria**

34.3 Countries could consider adopting measures to facilitate access by financial institutions to beneficial ownership and control information, so as to allow them to more easily verify the customer identification data.

## D. INTERNATIONAL CO-OPERATION

**Recommendation 35**

The criteria listed below should be read in conjunction with the texts of Recommendation 35 and Special Recommendation I, and the text of the Conventions referred to in Recommendation 35[54] (Note to assessors: Ensure that the assessments of Criterion 35.1 and Criterion I.1 (in SR.I) are consistent.)

**Essential criteria**

35.1 Countries should sign and ratify, or otherwise become a party to, and fully implement, the Vienna Convention, the Palermo Convention and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention).[55]

**Additional criteria**

35.2 Countries should consider signing, ratifying, or otherwise becoming a party to, and fully implementing other relevant international conventions such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

[54] Assessors should be satisfied that all the articles relevant to ML and FT are fully implemented.

[55] Assessors should be satisfied that the following relevant articles of the Vienna Convention (Articles 3-9), the Palermo Convention (Articles 6-7, 10-16, 18-20, 26-27, 31 and 34), and the Terrorist Financing Convention (Articles 2-18) are fully implemented.

## Recommendation 36

The criteria listed below should be read in conjunction with the text of Recommendation 36 and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criteria 36.1 – 36.6 and Criterion V.1 (in SR.V) are consistent.)

### Essential criteria

36.1 Countries should be able to provide the widest possible range of mutual legal assistance in AML/CFT investigations, prosecutions and related proceedings[56].

Mutual legal assistance includes assistance of the following nature: (i) the production or seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons; (ii) searches and seizures of financial institutions, other entities, and domiciles; (iii) the taking of evidence or statements from persons; (iv) effecting service of judicial documents; (v) providing originals or copies of relevant documents and records; and (vi) identification, freezing, seizure, or confiscation of assets laundered or intended to be laundered, the proceeds of ML and assets used for or intended to be used for FT, as well as the instrumentalities of such offences, and assets of corresponding value.

*[DG to review if minimum elements of MLA]*

36.1.1 There should be evidence (including statistics) of such assistance having been provided in a rapid, constructive and effective manner.

36.2 Mutual legal assistance should not be prohibited or made subject to unreasonable, disproportionate or unduly restrictive conditions.

Possible examples of such conditions (for which an assessment as to reasonableness, proportionality or restrictiveness should be made) could include: generally refusing to provide assistance on the grounds that judicial proceedings have not commenced in the requesting country; requiring a conviction before providing assistance; requiring a treaty before providing assistance.

36.3 There should be clear and efficient processes for the execution of mutual legal assistance requests.

Obstacles to an efficient execution of mutual legal assistance requests include: failure to take the appropriate measures in a timely way, and long delays in responding.

*[DG to consider if examples or unacceptable measures]*

36.4 A request for mutual legal assistance should not be refused on the sole ground that the offence is also considered to involve fiscal matters.

36.5 A request for mutual legal assistance should not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions [or DNFBP, except where the relevant information was obtained in circumstances where professional secrecy or legal professional privilege applies[57].] *[DG to consider references to DNFBP]*

---

[56] Investigations, prosecutions and related proceedings may be of a criminal, civil enforcement or administrative nature, and includes proceedings in relation to confiscation or provisional measures.

[57] See also Criteria 16.2

36.6 The powers of competent authorities required under R.28 should also be available for use in response to requests for mutual legal assistance.

**Additional criteria**

36.7 To avoid conflicts of jurisdiction, countries should consider 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.

36.8 Where this is consistent with the domestic framework, the powers of competent authorities required under R.28 should also be available for use when there is a direct request from foreign judicial or law enforcement authorities to domestic counterparts[58].

[58] "Counterparts" refers to the definition provided in criteria 40.1

## Recommendation 37

The criteria listed below should be read in conjunction with the text of Recommendation 37 and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criterion 37.1 and Criterion V.2 (in SR.V) are consistent.)

### Essential criteria

37.1 To the greatest extent possible, mutual legal assistance should be rendered in the absence of dual criminality, [in particular, for less intrusive and non compulsory measures.]

37.2 For extradition and those forms of mutual legal assistance where dual criminality is required, the requested state (that is rendering the assistance) should have no legal or practical impediment to rendering assistance where both countries criminalise the conduct underlying the offence. Technical differences between the laws in the requesting and requested states, such as differences in the manner in which each country categorises or denominates the offence should not pose an impediment to the provision of mutual legal assistance.

**Recommendation 38**

The criteria listed below should be read in conjunction with the text of Recommendation 38 and its Interpretative Note, and the text of Recommendation 3 and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criteria 38.1 – 38.3 and Criterion V.3 are consistent.)

**Essential criteria**

38.1 There should be appropriate laws and procedures to provide an effective and timely response to mutual legal assistance requests by foreign countries related to the identification, freezing, seizure, or confiscation of:

(a) laundered property from,
(b) proceeds from,
(c) instrumentalities used in, or
(d) instrumentalities intended for use in,

the commission of any ML, FT or other predicate offences.

38.2 The requirements in Criteria 38.1 should also be met where the request relates to property of corresponding value.

38.3 Countries should have arrangements for co-ordinating seizure and forfeiture actions with other countries.

**Additional criteria**

38.4 Countries should consider including authorising the sharing of confiscated assets between them when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

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

## Recommendation 39

The criteria listed below should be read in conjunction with the text of Recommendation 39.

### Essential criteria

39.1 Money laundering should be an extraditable offence. There should be laws and procedures to extradite individuals charged with a money laundering offence.

39.2 Countries should either:

a) extradite their own nationals or,
b) where a country does not extradite its own nationals 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. In such cases, the competent 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.

39.3 In cases where the extradition takes place and in cases where a country prosecutes its own national for offences committed in another country, countries should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of the prosecution.

39.4 Consistent with the principles of domestic law, countries should adopt measures or procedures that will allow extradition requests and proceedings relating to ML to be handled without undue delay.

### Additional criteria

39.5 Countries [should] consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

## Recommendation 40

The criteria listed below should be read in conjunction with the text of Recommendation 40 and its Interpretative Note, and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criteria 40.1 – 40.9 and Criterion V.5 (in SR.V) are consistent.)

### Essential criteria

40.1 Countries should ensure that their competent authorities[59] are able to provide the widest range of international cooperation to their foreign counterparts[60].

40.1.1 There should be evidence [(including statistics)] of such cooperation having been provided in a rapid, constructive and effective manner.

40.2 There should be clear and effective gateways, mechanisms or channels that will facilitate and allow for prompt and constructive exchanges of information directly between counterparts[61].

Examples of gateways, mechanisms or channels used in international cooperation and exchanges of information (other than MLA or extradition) include Bilateral or multilateral agreements or arrangements; Memorandum of Understanding (MOU); Memorandum of Agreement (MOA); Exchanges on the basis of reciprocity; and Exchanges through appropriate international or regional organisations or bodies such as Interpol or the Egmont Group of FIUs.

40.3. Such exchanges of information should be possible: (a) both spontaneously and upon request, and (b) in relation to both money laundering and the underlying predicate offences.

40.4 Countries should ensure that all their competent authorities are authorised to conduct inquiries on behalf of foreign counterparts.

40.4.1 In particular, countries should ensure that their FIU is authorised to make the following types of inquiries on behalf of foreign counterparts: (a) searching its own databases, including with respect to information related to suspicious transaction reports; (b) searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

40.5 [Countries should ensure that their law enforcement authorities; and where permitted by domestic law, other competent authorities are authorised to conduct investigations on behalf of foreign counterparts].

---

[59] "Competent authorities" refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

[60] "Foreign Counterparts" refers to the authorities in another country that exercise similar responsibilities and functions.

[61] Obstacles to a prompt and constructive exchange of information include failing to respond or take the appropriate measures in a timely way, and unreasonable delays in responding.

40.6 Exchanges of information should not be made subject to disproportionate or unduly restrictive conditions.

40.7 Requests for cooperation should not be refused on the sole ground that the request is also considered to involve fiscal matters.

40.8 Requests for cooperation should not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions [or DNFBP, except where the relevant information that is sought is held in circumstances where professional secrecy or legal professional privilege applies[62].]

40.9 Countries should establish controls and safeguards to ensure that information received by competent authorities is used only in an authorised manner. These controls and safeguards should be consistent with national provisions on privacy and data protection[63].

Information sharing may require clear agreements between competent authorities such as: the information exchanged is used only for the specific purpose for which the information was sought or provided; [information exchanged can only be disseminated to another agency or third party in a manner consistent with the terms of the request for information] [the information exchanged cannot be disseminated to another agency or third party a) without the prior consent of the authority that disclosed the information (such consent should not be unreasonably withheld and should be given in a timely manner)] and [b)] cannot be retained longer than it is necessary for the fulfilment of the purpose for which the information is to be used.

**Additional criteria**

40.10 Where permitted by fundamental domestic legal principles, the FIU should contact other competent authorities and financial institutions [or DNFBP] to obtain relevant information requested by a foreign counterpart FIU.

40.11 Countries [should consider] permitting a prompt and constructive exchange of information with non-counterparts and this co-operation may occur either directly or indirectly[64].

40.11.1 The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

[62] See also criteria 16.2

[63] This implies that, at a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving competent authority.

[64] The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority.

# EIGHT SPECIAL RECOMMENDATIONS - CRITERIA

## Special Recommendation I

The criteria listed below should be read in conjunction with the text of Special Recommendation I, Recommendation 35, Special Recommendations II, III and V, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), and the following United Nations Security Council Resolutions: S/RES/1267(1999), its successor resolutions 1333(2000), S/RES/1363(2001), S/RES/1390(2002) and S/RES/1455(2003), and S/RES/1373(2001). (Note to assessors: Ensure that the assessments of Criterion I.1 and Criterion 35.1 (in R.35) are consistent. Also ensure that the assessments of SR.I, SR.II, SR.III and SR.V are consistent.)

### Essential criteria

I.1 Countries should sign and ratify, or otherwise become a party to, and fully implement, the Terrorist Financing Convention.[65]

I.2 Countries should fully implement the United Nations Security Council Resolutions relating to the prevention and suppression of FT. These comprise S/RES/1267(1999), its successor resolutions S/RES/1333(2000), S/RES/1390(2002) and S/RES/1455(2003), S/RES/1363(2001) and S/RES/1373(2001). This requires any necessary laws / regulations or other measures to be in place and for these provisions to cover the requirements contained in those resolutions.

### Additional criteria

[I.3 Countries should consider signing, ratifying, or otherwise becoming a party to, and fully implementing other relevant international conventions such as the 2002 Inter-American Convention against Terrorism.]

[65] Assessors should be satisfied that all relevant articles of the Terrorist Financing Convention are fully implemented (Articles 2-6 and 17-18 which relate to SR.II; Article 8 which relates to SR.III; and Articles 7 and 9-18 which relate to SR.V.)

## Special Recommendation II

The criteria listed below should be read in conjunction with the text of Special Recommendation II, Special Recommendation I, Recommendations 1 and 2, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), the definitions of "terrorist act" and "terrorist organisation" in the Interpretative Note to Special Recommendation III and the definition of "funds" in Article 1 of the Terrorist Financing Convention. (Note to assessors: Ensure that the assessments of Criteria II.1 – II.3, Criterion I.1 (in SR.I) and Criteria 1.3 – 1.6 (in R.1) are consistent.)

## Essential Criteria

II.1 The financing of terrorism, terrorist acts and terrorist organisations (jointly referred to as terrorist financing or FT) should be criminalised on the basis of the Terrorist Financing Convention.[66,67] The offence of terrorist financing should extend to any funds as defined in the TF Convention[68]. *[DG to check consistency on definition of funds between SRIII and TF Convention]*

II.2 The offence of terrorist financing should be a predicate offence for money laundering.

II.3 The offence of terrorist financing should extend to situations where the person alleged to have committed the offence is in one country, but the terrorist(s), terrorist organisation(s), or place where the terrorist act(s) occurs is/are in another country.

II.4 Countries should ensure that Criteria 2.1 to 2.5 (in R.2) also apply in relation to the offence of FT.

II.5 Countries should ensure that Criterion 1.7 (in R.1) also applies in relation to the offence of FT.

---

[66] Article 2 of the Terrorist Financing Convention states:
"Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
(a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
(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 organization to do or to abstain from doing any act.

[67] [In order to comply with SR II, it is not sufficient to rely on ancillary offences that apply to terrorist offences e.g. aiding and abetting or conspiracy offences. This interpretation is consistent with the views of UNCTC experts.]

[68] Article 1 of the Terrorist Financing Convention defines *funds* as "assets 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 assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.

## Special Recommendation III

The criteria listed below should be read in conjunction with the text of Special Recommendation III, its Interpretative Note, its Best Practices Paper, Special Recommendation I, Recommendation 3, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), the following United Nations Security Council Resolutions: S/RES/1267(1999), its successor resolutions 1333(2000), S/RES/1363(2001), S/RES/1390(2002) and S/RES/1455(2003), S/RES/1373(2001) and S/RES/1452(2002), and the definitions of "confiscate", "designated person", "freeze", "funds or other assets", "seize", "S/RES/1267(1999)", "terrorist", "terrorist act", "terrorist organisation", "those who finance terrorism" and "without delay" in the Interpretative Note to SR.III. (Note to assessors: Ensure that the assessments of Criteria III.1 – III.12, Criteria I.1 – I.2 (in SR.I), Criteria VIII.2 (in SR.VIII) and Criteria 3.1 – 3.4 and Criterion 3.6 (in R.3) are consistent.)

### Essential criteria

*Freezing and, where appropriate, seizing under the relevant U.N. Resolutions:*

III.1 Countries should have effective laws and procedures to freeze terrorist funds or other assets of persons designated by the United Nations Al-Qaida and Taliban Sanctions Committee in accordance with S/RES/1267(1999)[69]. Such freezing should take place without delay and without prior notice to the designated persons involved.

III.2 A country should have effective laws and procedures to freeze terrorist funds or other assets of persons designated in the context of S/RES/1373(2001)[70]. Such freezing should take place without delay and without prior notice to the designated persons involved.

III.3 A country should have effective laws and procedures to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. Such procedures should ensure the prompt determination whether reasonable grounds or a reasonable basis exists to initiate a freezing action and the subsequent freezing of funds or other assets without delay upon determination, according to applicable national legal principles that a

---

[69] S/RES/1267(1999) and its successor resolutions—S/RES/1333(2000), S/RES/1363(2001), S/RES/1390(2002) and S/RES/1455(2003)—obligate countries to freeze without delay the funds or other assets owned or controlled by Al-Qaida, the Taliban, Usama bin Laden, or persons and entities associated with them as designated by the United Nations Al-Qaida and Taliban Sanctions Committee established pursuant to United Nations Security Council Resolution 1267(1999)., including funds derived from funds or other assets owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds or other assets are made available, directly or indirectly, for such persons' benefit, by their nationals or by any person within their territory. The Al-Qaida and Taliban Sanctions Committee is the authority responsible for designating the persons and entities that should have their funds or other assets frozen under S/RES/1267(1999) and its successor resolutions. All countries that are members of the United Nations are obligated by S/RES/1267(1999) and its successor resolutions to freeze the assets of persons and entities so designated by the Al-Qaida and Taliban Sanctions Committee.

[70] S/RES/1373(2001) obligates jurisdictions to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual jurisdiction has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective co-operation is developed among jurisdictions, jurisdictions should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. When (i) a specific notification or communication is sent and (ii) the jurisdiction 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 is a terrorist, one who finances terrorism or a terrorist organisation, the jurisdiction receiving the request must ensure that the funds or other assets of the designated person are frozen without delay.

requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that such grounds or basis for freezing exist.

III.4 The freezing actions referred to in Criteria III.1 – III.3 should extend to:

(a) funds or other assets wholly or jointly[71] owned or controlled, directly or indirectly, by designated persons, terrorists, those who finance terrorism or terrorist organisations; and

(b) funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons, terrorists, those who finance terrorism or terrorist organisations.

III.5 Countries should have effective systems for communicating actions [to be] taken under the freezing mechanisms referred to in Criteria III.1 – III.3 to the financial sector immediately upon taking such action. *[DG to consider mechanisms to communicate to the general public]*

III.6 Countries should provide clear guidance to financial institutions and other persons or entities that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms.

III.7 Countries should have effective and publicly-known procedures for considering de-listing requests and for unfreezing the funds or other assets of de-listed persons or entities in a timely manner consistent with international obligations.

III.8 Countries should have effective and publicly-known procedures for unfreezing, in a timely manner, the funds or other assets of persons or entities inadvertently affected by a freezing mechanism upon verification that the person or entity is not a designated person.

III.9 Countries should have appropriate procedures for authorising access to funds or other assets that were frozen pursuant to S/RES/1267(1999) and that have been determined to be necessary for basic expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses. These procedures should be in accordance with S/RES/1452(2002).

III.10 Countries should have appropriate procedures through which a person or entity whose funds or other assets have been frozen can challenge that measure with a view to having it reviewed by a court.

*Freezing, Seizing and Confiscation in other circumstances*

III.11 Countries should ensure that Criteria 3.1 – 3.4 and Criterion 3.6 (in R.3) also apply in relation to the freezing, seizing and confiscation of terrorist-related funds or other assets in contexts other than those described in Criteria III.1 – III.10.

*General provisions*

III.12 Laws and other measures should provide protection for the rights of bona fide third parties. Such protection should be consistent with the standards provided in Article 8 of the Terrorist Financing Convention, where applicable.

III.13 Countries should have appropriate measures to monitor effectively the compliance with relevant legislation, rules or regulations governing the obligations under SR III and to impose civil,

[71] "Jointly" refers to those assets held jointly between or among designated persons, terrorists, those who finance terrorism or terrorist organisations on the one hand, and a third party or parties on the other hand.

administrative or criminal sanctions for failure to comply with such legislation, rules or regulations.

**Additional criteria**

III.14 Countries should consider implementing the measures set out in the Best Practices Paper for SR.III.

III.15 Countries should consider implementing procedures to authorise access to funds or other assets that were frozen pursuant to S/RES/1373(2001) and that have been determined to be necessary for basic expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses. These procedures should be consistent with S/RES/1373(2001) and the spirit of S/RES/1452(2003).

## Special Recommendation IV

The criteria listed below should be read in conjunction with the texts of Special Recommendation IV, and Recommendations 13, 16 and 17. (Note to assessors: Ensure that the assessments of Criteria IV.1 – IV.4, Criteria 13.1 – 13.4 (in R.13), Criterion 16.1 – 16.3 (in R.16) and Criteria 17.1 – 17.4 (in R.17) are consistent.)

### Essential criteria

IV.1 A financial institution should be required by law or regulation to report to the FIU (a suspicious[72] transaction report – STR) when it suspects or has reasonable grounds to suspect that funds[73] are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism. This 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 FT offence or otherwise (so called "indirect reporting"), is not acceptable.

IV.2 Countries should ensure that Criteria 13.3 – 13.4 (in R.13) also apply in relation to the obligations under SR IV.

IV.3 Countries should ensure that Criteria IV.1 – IV.2 apply to DNFBP in the circumstances set out in Criterion 16.1 (in R.16), and subject to any qualifications under R.16.

IV.4 [Countries should ensure that Criteria 17.1 – 17.4 (in R.17) also apply in relation to the obligations under SR IV.
*[DG to review]*

### Additional criteria

IV.5 Countries should consider whether Criterion 16.4 should apply to DNFBP in the circumstances set out in Criterion 16.1 (in R.16), and subject to any qualifications under R.16.

---

[72] Systems based on the reporting of unusual transactions (rather than suspicious transactions) are equally satisfactory.

[73] *Funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable and legal documents or instruments evidencing title to, or interest in, such assets. (This definition of *funds* is also used in R.13.)

## Special Recommendation V

The criteria listed below should be read in conjunction with the texts of Special Recommendation V, Special Recommendation I, Recommendations 36-40, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), Special Recommendation III and the definition of "terrorist act" in the Interpretative Note to Special Recommendation III. (Note to assessors: Ensure that the assessments of Criteria V.1 – V.5, Criterion I.1 (in SR.I), Criteria 36.1 – 36.6 (in R.36), Criterion 37.1 (in R.37), Criteria 38.1 – 38.3 (in R.38) and Criteria 40.1 – 40.9 (in R.40) are consistent.)

### Essential criteria

V.1 Countries should ensure that Criteria 36.1 – 36.6 (in R.36) also apply to the obligations under SR.V.

V.2 Countries should ensure that Criterion 37.1 (in R.37) also applies to the obligations under SR.V.

V.3 Countries should ensure that Criteria 38.1 – 38.3 (in R.38) also apply to the obligations under SR.V.

V.4 Countries should ensure that Criteria 39.1 – 39.4 (in R.39) also apply to extradition proceedings related to terrorist acts and FT.

V.5 Countries should ensure that Criteria 40.1 – 40.9 (in R.40) also apply to the obligations under SR.V.

### Additional criteria

V.6 Countries should consider whether Criterion 36.7 – 36.8 (in R.36) should apply in relation to the obligations under SR.V.

V.7 Countries should consider whether Criterion 38.4 – 38.5 (in R.38) should apply in relation to the obligations under SR.V.

V.8 Countries should consider whether Criterion 39.5 (in R.39) should apply extradition proceedings related to terrorist acts or FT.

V.9 Countries should consider whether Criteria 40.10 – 40.11 (in R.40) should apply in relation to the obligations under SR.V.

## Special Recommendation VI

The criteria listed below should be read in conjunction with the text of Special Recommendation VI, its Interpretative Note and its Best Practices Paper, Special Recommendation VII and its Interpretative Note, Recommendation 17 and the definitions of "agent", "licensing", "money or value transfer service", and "registration" in the Interpretative Note to Special Recommendation VI. (Note to assessors: Ensure that the assessments of Criterion VI.5 and Criteria 17.1 – 17.4 (in R.17) are consistent.)

### Essential criteria

VI.1 Countries should designate a competent authority to register and/or licence natural and legal persons that perform money or value transfer services (MVT service operators), maintain a current list of the names and addresses of licensed and/or registered MVT service operators, and be responsible for ensuring compliance with licensing and/or registration requirements.[74]

VI.2 Countries should ensure that all MVT service operators are subject to the applicable FATF Forty Recommendations (in particular Recommendations 4-11, 13-15 and 21-23) and FATF Eight Special Recommendations (in particular SR.VII).

VI.3 Countries should have systems in place for monitoring licensed/registered MVT service operators and ensuring that they comply with the FATF Recommendations.

VI.4 Countries should require each licensed or registered MVT service operator to maintain a current list of its agents and to provide that list to the designated competent authority.

VI.5 Countries should ensure that Criteria 17.1 – 17.4 (in R.17) also apply in relation to the obligations under SR VI.

### Additional Criteria

VI.6 Countries should consider implementing the measures that are set out in the Best Practices Paper for SR VI.

[74] SR.VI does not require countries to establish a separate licensing/registration system or designate another competent authority in respect of money remitters which are already licensed/registered as financial institutions within the country, permitted to perform MVT services under the terms of their license/registration, and already subject to the full range of applicable obligations under the FATF Forty Recommendations and Eight Special Recommendations.

## Special Recommendation VII

The criteria listed below should be read in conjunction with the text of SR.VII and its Interpretative Note, Recommendations 5 and 17, and the definitions of "cross-border transfer", "domestic transfer", "financial institution", "funds transfer", "originator" and "wire transfer" in the Interpretative Note to Special Recommendation VII. (Note to assessors: Ensure that the assessments of Criterion VII.1, VII.9, Criteria 5.2 – 5.3 (in R.5) and Criteria 17.1 – 17.4 (in R.17) are consistent.)

### Essential criteria

SR VII 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 card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by SR VII, 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.

VII.1 For cross-border wire transfers (including batch transfers[75] and transactions using a credit or debit card to effect a funds transfer[76]), the ordering financial institution should be required to include the following *originator* information, verified for accuracy in accordance with Criteria 5.3 (in R.5), in the message or payment form accompanying the wire transfer:

- the name of the originator;
- the originator's account number (or a unique reference number if no account number exists); and
- the originator's address (countries may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth).

If a cross-border wire transfer is contained within a batch transfer and is sent by a financial institution, it may be treated as a domestic wire transfer. However, if it is sent through a money/value transfer service[77] (i.e. a money remitter), it must be treated as a cross-border wire transfer.

These requirements do not apply to: (a) credit or debit card transactions if the credit or debit card number accompanies all wire transfers that flow from the transaction; and (b) transfers and settlements between financial institutions where both the originator and beneficiary are financial institutions acting on their own behalf.

VII.2 For domestic wire transfers (including transactions using a credit or debit card as a payment system to effect a money transfer), the ordering financial institution should be required to comply with Criteria VII.1 above or it may include only the originator's account number or a unique identifier provided that the originator information referred to above can be made available to the

---

[75] A *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.

[76] This example relates to new products, such as those developed by Visa and Mastercard, which allow debit or credit cards to be used to effect wire transfers through a proprietary system. This example does not refer to conventional debit or credit card transfers (such as withdrawals from a bank account through an ATM machine, cash advances from a credit card, or payments for goods and services) which are exempt from SR VII.

beneficiary financial institution/competent authorities within three business days of receiving a request, and domestic law enforcement authorities can compel immediate production of it.

These requirements do not apply to: (a) credit or debit card transactions if the credit or debit card number accompanies all wire transfers that flow from the transaction; and (b) transfers and settlements between financial institutions where both the originator and beneficiary are financial institutions acting on their own behalf.

VII.3 Financial institutions should be required to ensure that only routine wire transfers are sent in batch transfers. Financial institutions should not batch wire transfers that are not routine or carry an increased risk of being related to money laundering or terrorist financing.

The following is a typical example of a routine batch transfer. Every month, Financial Institution A sends 100 wire transfers relating to pension/social security/dividend payments etc. to 100 customers of Financial Institution B. Financial Institution A sends all 100 wire transfers to Financial Institution B in a single batch rather than sending them each individually. Because of the routine nature of these wire transfers, there is little risk that they are related to ML/FT.

VII.4 Each intermediary financial institution in the payment chain should be required to maintain all the required originator information with the accompanying wire transfer.[78]

VII.5 If the country has a *de minimis* threshold in place, that threshold must not be above USD 3,000.[79] Notwithstanding any thresholds, accurate and meaningful originator information must be retained and made available by the ordering financial institution as set forth in Criterion VII.1.

VII.7 Beneficiary financial institutions should adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information.

An example of a procedure for handling such wire transfers would be to:

- Request the missing originator information from the financial institution that sent the wire transfer.
- If the missing information is not forthcoming, consider whether, in all the circumstances, the absence of complete originator information creates or contributes to suspicion about the wire transfer or a related transaction. If the wire transfer is deemed to be suspicious, then it should be reported to the FIU. In addition, the institution may decide not to accept the wire transfer.
- In appropriate circumstances, beneficiary financial institutions should consider restricting or terminating business relationships with financial institutions that do not comply with SR VII. In this regard, evaluators/assessors could also refer to the criteria for R.5 (Criteria 5.14 – 5.15).

[78] However, where technical limitations prevent the full originator information accompanying a cross border wire transfer from remaining with a related domestic wire transfer, a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution. This option is only possible until 14 February 2005.

[79] Jurisdictions may have a *de minimis* threshold (no higher than USD 3,000) [until the FATF has completed its review of the appropriateness of the threshold. The FATF will undertake such a review commencing in February 2004. Where a de minimis threshold exists in a country, assessors should examine the appropriateness of that threshold.]

VII.8 Countries should have measures in place to effectively monitor the compliance of financial institutions with rules and regulations implementing SR.VII.

VII.9 Countries should ensure that Criteria 17.1 – 17.4 (in R.17) also apply in relation to the obligations under SR.VII.

## Special Recommendation VIII

The criteria listed below should be read in conjunction with the text of Special Recommendation VIII, its Best Practices Paper, the definition of "non-profit organisation" in paragraphs 2 – 3 of the Best Practices Paper to SR.VIII, Special Recommendation III, and the definitions of "freeze", "funds or other assets", "seize", "terrorist" and "terrorist organisation" in the Interpretative Note to SR.III. (Note to assessors: Ensure that the assessments of Criterion VIII.2 and Criteria III.1 – III.13 (in SR III) are consistent.

### Essential criteria

In implementing the criteria below, countries may take a risk based approach taking into account, for example, the size of the organisation, the amount of funds it handles, and its specific objectives.

VIII.1 Countries should review the adequacy of laws and regulations that relate to non-profit organizations that can be abused for the financing of terrorism. There should be evidence available to assessors that this review has taken place.

VIII.2. Countries should have measures in place to ensure that terrorist organisations cannot pose as legitimate non-profit organisations, including for the purpose of escaping asset freezing or seizing measures.

VIII.3 Countries should have measures in place to ensure that funds or other assets collected by or transferred through non-profit organizations are not diverted to support the activities of terrorists or terrorist organisations.

Examples of possible measures (drawn from the Best Practices Paper to Special Recommendation VIII) include:

- Oversight on the non-profit sector that is flexible, effective, and proportional to the risk of abuse by terrorists
- Record-keeping and reporting policies to enhance the financial transparency of non-profit organisations
- Having an ability to verify that funds have been spent as advertised and planned
- Requiring non-profit organisations to document their administrative, managerial and policy control over their operations
- Effective coordination between non-profit sector oversight/regulatory bodies, law enforcement and security agencies, FIUs, and financial system regulators.
- Guidance to financial institutions with regard to CDD and suspicious transaction reporting where the client is an NPO.

### Additional criteria

VIII.4 Countries could consider implementing the measures set out in the Best Practices Paper for SR.VIII.

**Annex 1**

**Aide-memoire to assessors**
**Types of Financial Institutions covered by the 40+ 8 Recommendations**

*[DG to review contents and formatting. Issue of lawyers and DNFBP. Add note to assessors]*

| Financial Activity | Examples of types of financial institutions that engage in the activity |
|---|---|
| 1. Acceptance of deposits and other repayable funds from the public. | Banks, credit unions, building societies, savings and loan institutions. |
| 2. Lending. | Banks, Mortgage lending company, finance company, [factoring company] |
| 3. Financial leasing. | Leasing companies for non-consumer products |
| 4. The transfer of money or value. | Money remittance businesses (MVT service operators, both formal and informal) |
| 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). | Payment companies |
| 6. Financial guarantees and commitments. | Banks etc |
| 7. Trading in:<br>(a) money market instruments (cheques, bills, CDs, derivatives etc.);<br>(b) foreign exchange;<br>(c) exchange, interest rate and index instruments;<br>(d) transferable securities;<br>(e) commodity futures trading. | Brokers (market intermediaries) |
| 8. Participation in securities issues and the provision of financial services related to such issues. | Brokers (market intermediaries), investment banks |
| 9. Individual and collective portfolio management. | Covers management of collective investment schemes such as unit trusts, mutual funds, private pension funds |
| 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. | Custodians |
| 11. Otherwise investing, administering or managing funds or money on behalf of other persons. | Could apply to FI mentioned above, |
| 12.Underwriting and placement of life insurance and other investment related insurance. | Life insurance companies, agents and brokers. Also cover other investment linked insurance. Application to viatical settlements? [A viatical settlement is a lump sump given to terminally ill people (viators) in exchange for the death benefits of their life insurance. |
| 13.Money and currency changing. | Bureaux de change, money exchange business |

**Annex 2**

## DEFINITIONS USED IN THE METHODOLOGY - THE 40 RECOMMENDATIONS

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Beneficial owner* | *Beneficial owner* refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement. | Glossary | R.5, 6, 21, 23, 24, 33, and 34 |
| *Bearer shares* | *Bearer shares* refers to negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate. | OECD Report of April 2001 on "Using Corporate Entities for Illicit Purposes" | R.33 |
| *Competent authorities* | *Competent authorities* refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors. | IN of R.40 | Applicable to R.40 |
| *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. | Glossary | R. 23 |
| *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 of funds, cheque clearing, payable-through accounts and foreign exchange services. | | R.7 and 18 |
| *Designated categories of offences* | *Designated categories of offences* means:<br>• participation in an organised criminal group and racketeering;<br>• terrorism, including terrorist financing;<br>• trafficking in human beings and migrant smuggling;<br>• sexual exploitation, including sexual exploitation of | Glossary | R.1 |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| | children;<br>• illicit trafficking in narcotic drugs and psychotropic substances;<br>• illicit arms trafficking;<br>• illicit trafficking in stolen and other goods;<br>• corruption and bribery;<br>• fraud;<br>• counterfeiting currency;<br>• counterfeiting and piracy of products;<br>• environmental crime;<br>• murder, grievous bodily injury;<br>• kidnapping, illegal restraint and hostage-taking;<br>• robbery or theft;<br>• smuggling;<br>• extortion;<br>• forgery;<br>• piracy; and<br>• insider trading and market manipulation.<br><br>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:***<br>***a) Casinos (which also includes internet casinos).***<br>***b) Real estate agents.***<br>***c) Dealers in precious metals.***<br>***d) Dealers in precious stones.***<br>***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 measures that would combat money laundering.***<br>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:<br><br>• acting as a formation agent of legal persons;<br>• acting as (or arranging for another person to act as) a director or secretary of a company, a | Glossary | R. 4, 5, 12, 16, 17, 20, 24, 25, 31, 32, 36, 40 and SR IV |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| | partner of a partnership, or a similar position in relation to other legal persons;<br>• providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;<br>• acting as (or arranging for another person to act as) a trustee of an express trust;<br>• acting as (or arranging for another person to act as) a nominee shareholder for another person. | | |
| *Designated threshold* | *Designated threshold* refers to the amount set out in the Interpretative Notes. | Glossary | R.5, 12 and16 |
| *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 e.g. constructive trust. | | R.12, 16 and 34 |
| *Financial institutions* | *Financial institutions* means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:<br>1. Acceptance of deposits and other repayable funds from the public.[80]<br>2. Lending.[81]<br>3. Financial leasing.[82]<br>4. The transfer of money or value.[83]<br>5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).<br>6. Financial guarantees and commitments.<br>7. Trading in:<br>(a) money market instruments (cheques, bills, CDs, | Glossary | R.4-6, 11, 14-18, 21-23, 25, 26, 28-30, 33, 34, 36, 40, SRIII, SRIV, SRVI and SRVII |

[80] This also captures private banking.

[81] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).

[82] This does not extend to financial leasing arrangements in relation to consumer products.

[83] This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. 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 Interpretative Note to Special Recommendation VII.

[84] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| | derivatives etc.);<br>(b) foreign exchange;<br>(c) exchange, interest rate and index instruments;<br>(d) transferable securities;<br>(e) commodity futures trading.<br>8. Participation in securities issues and the provision of financial services related to such issues.<br>9. Individual and collective portfolio management.<br>10. Safekeeping and administration of cash or liquid securities on behalf of other persons.<br>11. Otherwise investing, administering or managing funds or money on behalf of other persons.<br>12. Underwriting and placement of life insurance and other investment related insurance[84].<br>13. Money and currency changing.<br>When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.<br>In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above. | | |
| *FIU* | FIU means financial intelligence unit. | Glossary | R.3, 13, 14, 16, 17, 21, 25-27, 30-32, 40, SRIV and SR VII |
| *Foreign counterparts* | *Foreign counterparts* refers to the authorities in another country that exercise similar responsibilities and functions. | IN of R.40 | Applicable to the criteria under R.40 |
| *Funds* | *Funds* refers to assets of every kind, [whether corporeal or incorporeal, tangible or intangible, movable or immovable and legal documents or instruments evidencing title to, or interest in, such assets]. | | R.13 and 27 |
| *Legal arrangements* | *Legal arrangements* refers to express trusts or other similar legal arrangements. Examples of other similar arrangements | Glossary. | R.5, 15 and 34 |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| | (for AML/CFT purposes) include fiducie, treuhand and fideicomiso. | | |
| *Legal persons* | *Legal persons* refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property. | Glossary | R.2, 5, 12, 15-17, 21, 33, 36 and SR VI |
| *Payable-through accounts* | *Payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf. | Glossary | R.7 |
| *Politically Exposed Persons" (PEPs)* | *PEPs* are individuals who are or have been entrusted with prominent public functions in 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. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. | Glossary | R.6 |
| *Proceeds* | *Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence. | Palermo Convention | R.1, 3, 13, 27, 28, 30, 35, 36 & 38 |
| *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. | Palermo Convention | R.1, 3, 30, 32, and 38 |
| *Self-regulatory organisation (SRO)* | A *SRO* is a body that represents the profession, and which is made up of member professionals, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory type functions. For example, it would be normal for this body to enforce rules to ensure that high ethical and moral standards are maintained by those practicing the profession. | | R.16 and 24 |
| *Settlor* | *Settlors* are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets. | | R.7 and 34 |
| *Shell bank* | *Shell bank* means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group. | Glossary | R.18 |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *STR* | *STR* refers to suspicious transaction reports. | Glossary | R.13, 14, 16, 26 & 27 and SRIV |
| *Supervisors* | *Supervisors* refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing. | Glossary | R.17, 21, 23, 29, 30-32 and 40 |
| *The FATF Recommendations* | *The FATF Recommendations* refers to these Recommendations and to the FATF Special Recommendations on Terrorist Financing. | Glossary | R.4, 5, 9, 17, 21-24, 29 and SRVI |
| *Trustee* | *Trustees*, who may be paid professionals or companies or unpaid persons, hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes. There may also be a protector, who may have power to veto the trustees' proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees. | | R. 5, 12, 16 and 34 |

**Annex 3**

## DEFINITIONS USED IN THE METHODOLOGY - THE 8 SPECIAL RECOMMENDATIONS

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Agent* | An *agent* is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires). (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.) | INSR.VI | Definitions of "DNFBP" and "financial institution", R.9, 12, 16 and SR.VI |
| *Confiscate* | The term *confiscate,* 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.) (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III.) | INSR.III | R.28, 30, 32, 38 and SR.III |
| *Cross-border transfer* | *Cross-border transfer* means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | INSR.VII |
| *Designated person* | The term *designated persons* refers to those persons or entities designated by the Al-Qaida and Taliban Sanctions Committee pursuant to S/RES/1267(1999) or those persons or entities designated and accepted, as appropriate, by jurisdictions pursuant to S/RES/1373(2001). (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III.) | INSR.III | INSR.III |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Domestic transfer* | *Domestic transfer* means any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | INSR.VII |
| *Financial institution* | The term *financial institution* is as defined by the FATF Forty Recommendations (2003). The term does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | Definition of "financial institution",<br><br>R.4-18, 21-23, 25-26, 28-30, 32-34, 36, 40, SR.III, IV, VI andVII |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Freeze* | *Freeze* means to prohibit the transfer, conversion, disposition or movement of funds or other assets 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. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the freezing and may continue to be administered by the financial institution or other arrangements designated by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III ans SR.VIII.) | INSR.III | R.3, 27-28, 30, 32, 36, 38 and SR.III and VIII |
| *Funds or other assets* | The term *funds or other assets* means financial assets, 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. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III and SR.VIII.) | INSR.III | Definition of "financial institutions",<br><br>R.5-7, 13, 27 and SR.II, III, IV, VII and VIII |
| *Funds transfer* | The terms *funds transfer* refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | SR.VII |
| *Licensing* | *Licensing* means a requirement to obtain permission from a designated competent authority in order to operate a money/value transfer service legally. (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.) | INSR.VI | R.17, 23 and SR.VI |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Money or value transfer service* | *Money or value transfer service* refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.<br><br>A money or value transfer service may be provided by persons (natural or legal) formally through the regulated financial system or informally through non-bank financial institutions or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or *underground* (or *parallel) banking systems*. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala, hundi, fei-chien,* and the *black market peso exchange*. (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.) | INSR.VI | R.23 and SR.VI |
| *Non-profit organisations* | Non-profit organisations can take on a variety of forms, depending on the jurisdiction and legal system. Within FATF members, law and practice recognise associations, foundations, fund-raising committees, community service organisations, corporations of public interest, limited companies, Public Benevolent Institutions, all as legitimate forms of non-profit organisation, just to name a few.<br><br>This variety of legal forms, as well as the adoption of a risk-based approach to the problem, militates in favour of a functional, rather than a legalistic definition. Accordingly, the FATF has developed suggested practices that would best aid authorities to protect non-profit organisations **that engage in raising or disbursing funds** for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works" from being misused or exploited by the financiers of terrorism. (This definition is drawn from the Best Practices Paper to SR.VIII. It is used in the criteria under SR.VIII.) | BPP.VIII | SR.VIII |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Originator* | The *originator* is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | SR.VII |
| *Registration* | *Registration* in this Recommendation means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally. (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.) | INSR.VI | R.17, 33, 34 and SR.VI |
| *Seize* | The term *seize* means to prohibit the transfer, conversion, disposition or movement of funds or other assets 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 funds or other assets. The seized funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized funds or other assets. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III and SR.VIII.) | INSR.III | R.3, 27-28, 30, 32, 36, 38 and SR.III and VIII |
| *S/RES/1267(1999)* | The term *S/RES/1267(1999)* refers to S/RES/1267(1999) and its successor resolutions. When issued, S/RES/1267(1999) had a time limit of one year. A series of resolutions have been issued by the United Nations Security Council (UNSC) to extend and further refine provisions of S/RES/1267(1999). By successor resolutions are meant those resolutions that extend and are directly related to the original resolution S/RES/1267(1999). As of November 2003, these resolutions included S/RES/1333(2000), S/RES/1363(2001), S/RES/1390(2002) and S/RES/1455(2003). (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.I and SR.III. It is used in the criteria under SR.III.) | INSR.III | SR.I and III |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *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 or terrorist financing; (iii) organises or directs others to commit terrorist acts or terrorist financing; or (iv) contributes to the commission of terrorist acts or terrorist financing 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 terrorist financing or with the knowledge of the intention of the group to commit a terrorist act or terrorist financing. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III and SR.VIII.) | INSR.III | SR.II, III and VIII |
| *Terrorist act* | A *terrorist act* includes an act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft, Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, International Convention against the Taking of Hostages, Convention on the Physical Protection of Nuclear Material, 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, Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, International Convention for the Suppression of Terrorist Bombings, and the International Convention for the Suppression of the Financing of Terrorism (1999). (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.II, SR.III, SR.V.) | INSR.III | R.13 and SR.II, III, IV and V |
| *Terrorist organisation* | The term *terrorist organisation* refers to any legal person, group, undertaking or other entity owned or controlled directly or indirectly by a terrorist(s). (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.II, SR.III and SR.VIII.) | INSR.III | R.13 and SR.II, III, IV and VIII |

| Terms | Definition | Where Term is Defined | Where Term is Used |
|---|---|---|---|
| *Those who finance terrorism* | The phrase *those who finance terrorism* refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III.) | INSR.III | R.13 and SR.III and IV |
| *Without delay* | The phrase *without delay,* for the purposes of S/RES/1267(1999), means, ideally, within a matter of hours of a designation by the Al-Qaida and Taliban 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. The phrase *without delay* should be interpreted in the context of the need to prevent the flight or dissipation of terrorist-linked funds or other assets, and the need for global, concerted action to interdict and disrupt their flow swiftly. (This definition is drawn from the Interpretative Note to SR.III. It is used in the criteria under SR.III.) | INSR.III | R.9 and SR.III |
| *Wire transfer* | The terms *wire transfer* refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person. (This definition is drawn from the Interpretative Note to SR.VII. It is used in the criteria under SR.VII.) | INSR.VII | R.5, 7, 12, 32 and SR.VII |

**NOTE:** This list does not include the following definitions which are also used in the assessment of the Eight Special Recommendations:

- *batch transfer* (as used in the criteria under SR.VII);
- *funds* (as defined in Article 1 of the Terrorist Financing Convention and used in the criteria under SR.II); or