Financial Action Task Force

Groupe d'action financière

AML/CFT Evaluations and Assessments

Handbook for Countries and Assessors

June 2007

Table of Contents

Introduction

1. This handbook is intended to the assist assessment teams and the examined countries that are participating in an Anti-Money Laundering/Combating Terrorist Financing (AML/CFT) mutual evaluation carried out by the FATF or an FSRB[1] (FATF style regional body) or taking part in an IMF/World Bank assessment. It provides both procedural information and detailed instructions for performing a proper and fair evaluation/assessment.

2. The FATF has already issued a key instrument to guide the assessment of a country's compliance with the international AML/CFT standards, *the Anti-Money Laundering/Combating Terrorist Financing Methodology 2004* which was adopted by the FATF in February 2004 and endorsed by the Executive Boards of the IMF and the World Bank in March 2004. The Methodology was amended by the FATF in February 2005 to bring it into line with the amended FATF Recommendations. The Methodology 2004 as amended from time to time (henceforth referred to as the "2004 Methodology"), which reflects the principles set out in the FATF Forty Recommendations 2003 and the FATF Nine Special Recommendations on Terrorist Financing 2001, provides a detailed description of what is necessary for an AML/CFT system. In the perspective of a new round of evaluations/assessments based on the FATF 40 + 9 Recommendations and the Methodology 2004, which started in 2005, the FATF has also prepared common documents such as a template of the mutual evaluation questionnaire, a template of the mutual evaluation report and an outline of the executive summary of the report.

3. The 2004 Methodology and the common documents are intended to be used by a number of different organisations, bodies and assessors and across a very significant number of countries. This handbook sets out instructions to assist individual assessors and examined countries on both substantive and procedural issues. It is also intended to help produce high standard reports and ensure a level playing field, i.e. the production of objective and consistent reports and summaries. Assessors will still have to exercise their judgement in determining whether a particular measure adopted by a country satisfies the criteria against which it is being assessed.

I. Key documents to be used by assessors and examined countries

(a) The FATF Forty Recommendations 2003 and the FATF Nine Special Recommendations on Terrorist Financing 2001.

(b) The Anti-Money Laundering/Combating Terrorist Financing (AML/CFT) Methodology 2004

4. The 2004 Methodology is a key tool to assist assessors when they are preparing AML/CFT mutual evaluation reports. It is designed to help them identify the key elements of the systems and mechanisms developed by countries with diverse legal, regulatory and financial frameworks.

5. The 2004 Methodology also provides general guidance to assessors when conducting the evaluation/assessment, particularly on the following topics:

[1] For the purpose of this handbook, references to an FSRB also include the Offshore Group of Banking Supervisors (OGBS). All AML/CFT references to mutual evaluations questionnaires and reports should be read as applying equally to the assessment questionnaires and detailed assessment reports used by the IMF and the World Bank.

- Analysis of compliance: essential criteria (mandatory elements of each Recommendation) vs. additional elements (non-mandatory elements of each Recommendation) and compliance ratings;
- Effective implementation (as a full component of the evaluation reflected in the compliance ratings); and
- Risk of money laundering or terrorist financing.

6. There is also an annex to the 2004 Methodology that sets out definitions or meanings for many of the words or phrases that are used in the document.

(c) The Mutual Evaluation Questionnaire (MEQ) – See Template at Annex 1

7. This questionnaire is the means by which the authorities in the country[2] being evaluated can provide all the detailed input to the evaluation/assessment process prior to the on-site mission. This input should describe (i) the measures that are currently in place, including the implementation measures and the results obtained, and (ii) the measures or changes which are not yet in place, but which the country has firm plans to implement (*"Description"* section). The response should clearly distinguish between measures in place and those that are planned. The country may also set out any additional analysis or commentary that it believes would assist the assessors in carrying out the evaluation/assessment e.g. its analysis of the effectiveness of the measures in place ("*Comments or other supplementary information"* section).

8. In their response to the mutual evaluation questionnaire, examined countries should provide a comprehensive description of the applicable measures for particular topic areas. At a minimum, the description should cover:

- all the essential criteria set out in the Methodology, i.e. all mandatory elements of the Recommendations;
- the additional elements set out in the Methodology, i.e. the non-mandatory elements of the Methodology that a country may have adopted. The level of detail provided with regard to the additional elements may vary depending on the issue and the approach adopted in a given country;
- any other relevant measures adopted that may help to describe and understand the system in place;
- citations, quotes or summaries sufficient to describe the relevant elements of the law or other measures.

(d) The Mutual Evaluation Report (MER) – See Template at Annex 2

9. The mutual evaluation report sets out the detailed findings on a country's AML/CFT regime and gives an assessment of compliance with the FATF 40 + 9 Recommendations. It also provides general information on the examined country and gives an overview on surrounding issues that help to define the context within which the AML/CFT regime operates (e.g. the government's strategy to prevent money laundering and terrorist financing the structure of the financial sector and a description of the types of designated non-financial businesses and professions (DNFBP) operating in the country).

(e) The Executive Summary of the MER – See Template at Annex 2

10. The Executive Summary should be the only summary of the MER, and provides the text for any summary that may be published. For the purposes of the preparation of the Report on Standards and Codes (ROSC), which are issued by the IMF and World Bank, the substantive text of the Executive

[2] All references to "country" also include territories or jurisdictions.

Summary should remain unchanged, but certain formal paragraphs should be added, as well as Table 2 Recommended Action Plan.

(f) Other key reference documents

11. Examined countries and assessors should have access to the following type of documents:

- international conventions, e.g. 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) and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism;
- relevant United Nations Security Council Resolutions, e.g. S/RES/1267(1999) and its successor resolutions and S/RES/1373(2001);
- the Core Principles and guidance issued by the Basel Committee, IOSCO or IAIS;
- Egmont Group Statement of Purpose and its Best Practices for the Improvement of Exchange of Information Between FIU.

12. Both examined countries and assessors should be familiar with the documents referred to in the Methodology 2004 (e.g. international conventions, UN Resolutions, etc.).

II. Composition of evaluation/assessment teams

13. The assessment of a country's AML/CFT system and its compliance with AML/CFT standards should be conducted by experts experienced in the legal, financial sector and law enforcement areas of AML/CFT systems. The process of assessing the essential criteria of the 2004 Methodology requires a judgmental weighing of numerous elements that only qualified assessors with practical, relevant experience can provide.

14. For FATF, a typical assessment team will consist of four experts who should come from different countries, and whose expertise must cover all aspects of the fight against money laundering and the financing of terrorism. For larger or more complex jurisdictions, additional experts could be required. Each evaluation/assessment team should therefore be comprised of: a legal expert (a judge, a prosecutor or a Ministry of Justice representative); two financial experts[3] (experts in regulatory matters: from a Finance Ministry, a Central Bank or a regulatory authority. Expertise regarding the preventive measures is necessary both for the financial sector and for the experts in preventive measures applied by designated non-financial businesses and professions); and a law enforcement expert (from operational services such as the police, customs or a financial intelligence unit).

15. Other bodies may have slightly different compositions for the assessment team though in all cases there should be at least one of each type of expert.

III. Assignment of primary responsibilities

16. Because the assessment of an AML/CFT regime requires a combination of financial, legal and law enforcement expertise, an AML/CFT evaluation/assessment needs to be undertaken by the experts in a fully collaborative process, and where all aspects of the review are conducted at the same time.

[3] The text refers to " financial expert(s)" as a shorthand description of the person(s) primarily responsible for examining the preventive measures such as customer due diligence, record keeping, suspicious transactions reporting (in collaboration with the law enforcement expert), internal controls, supervision or monitoring, etc. This responsibility applies to both the preventive measures for the financial sector and for the DNFBP.

17. Within this fully collaborative process, each of the experts is entitled to contribute to all parts of the review. However, each of the experts should take the lead on or take primary responsibility for topics related to his or her own area of expertise[4]:

a) the legal expert will take the lead in completing the MER sections on the legal system (Sections 2.1 to 2.4) and international co-operation (Sections 6.2 to 6.4);
b) the financial experts will take the lead in completing the MER sections related to the preventive measures for financial institutions (Section 3) and for DNFBP (Section 4);
c) the law enforcement expert will be responsible for completing the MER sections on the adequacy of implementation of the law enforcement measures (Sections 2.5 to 2.7);
d) all assessors will be responsible for assessing the adequacy of the measures in place for legal persons and arrangements and non-profit organisations (Section 5); for national co-operation and coordination (Section 6.1) and other forms of international co-operation (Section 6.5).

18. The Secretariats of the FATF and FSRBs will contribute to any parts of the mutual evaluation report to assist the assessors as necessary, and will be responsible for ensuring consistency between reports.

IV. The mutual evaluation/assessment process

19. Countries that have evaluations or assessments should be subject to a transparent and fair process with equality of treatment and a consistency of approach. Countries should commit themselves to provide timely and comprehensive responses to the MEQ and participate positively throughout the process of the evaluation/assessment. By agreeing to participate in this process, assessors undertake to provide timely and complete reports or responses. Both assessors and examined countries should meet the necessary deadlines in order to minimise the time between the dates of the on-site visit and the finalisation for the MER and the summary.

20. Assessors should be fully aware of the significant workload that is involved in participating in a mutual evaluation/assessment and must take into account relative to their own national commitments. The evaluation/assessment process requires a significant commitment, before, during and after the on-site visit and in the period leading to the finalisation of the MER. Assessors must also be able to attend the relevant FATF/FSRB Plenary meeting where the report is discussed. While this requires a significant input from the assessor, countries providing assessors should bear in mind that the process can also be very valuable for the country of the assessor.

V. Instructions for completing the mutual evaluation questionnaire

21. Examined countries should insert the appropriate detailed responses (both in the "Description" and in the "Comments or other supplementary information" sections) for Sections 2 to 7 of the MEQ. The MEQ lists all the criteria of the 2004 Methodology and countries should set out the relevant measures applicable to each criterion. Responses should be formulated broadly, fully describing all

[4] The breakdown is intended as a general guide. Each expert is able to contribute to each topic where their own expertise is relevant. For example, the FIU expert could contribute to the issue of STR (Sections 3.6, 3.7 & 4.2, 4.3) or the legal expert could assist in any area concerning interpretation of laws and regulations e.g. financial sector laws.

relevant measures in place for each Recommendation. Responses to the MEQ together with copies of all relevant laws, regulations and other documents[5] (in line with the instructions given in paragraph 9) should be made available to the assessment team two months before the on site-visit The questionnaire response should provide a description of all the elements of the AML/CFT system, including the implementation measures and the results obtained.

22. Examples of relevant laws, regulations and other documents that examined countries should provide are as follows:

- the laws applicable to the offences of money laundering and financing of terrorism, the provisions in relation to the predicate offences and any other laws or regulations dealing with the criminalisation of money laundering and terrorist financing;
- the laws, regulations and procedures applicable to the confiscation, seizing and freezing of the proceeds of crime, and to freezing terrorist funds in accordance with the United Nations Security Council Resolution;
- the laws establishing confidentiality or professional secrecy, applicable to financial institutions and DNFBP, including laws on legal professional privilege or legal professional secrecy applicable to the DNFBP;
- any laws imposing confidentiality or secrecy obligations on competent authorities and their staff should be provided;
- the laws, regulations and/or guidance notes governing financial institutions AML/CFT requirements, their supervision and the enforcement tools available to financial institution supervisors;
- the laws, regulations and/or guidance notes governing AML/CFT requirements of the DNFBP, their supervision/monitoring regime and the enforcement tools available to competent authorities;
- the laws and/or regulations establishing or governing the operations and conduct of the FIU;
- the laws and/or regulations on reporting of suspicious transactions, reports of large currency transactions or cross-border transportation of currency;
- the laws and/or regulations governing the money laundering and terrorist financing investigations and powers of law enforcement authorities or prosecution authorities;
- a description of the general regulatory/supervisory infrastructure for financial institutions and DNFPB including details of organisations staffing and budget;
- the AML/CFT provisions applicable to legal persons, legal arrangements and non-profit organisations;
- the relevant laws and/or regulations in relation to international co-operation, i.e. the ratification of international Conventions, mutual legal assistance and extradition;
- the laws and/or regulations governing other forms of international cooperation and information sharing by competent authorities;
- information on relevant bilateral and multilateral treaties, MOUs or other agreements relevant to international co-operation;
- any other guidance notes or other guidelines with AML/CFT purposes;
- reports filed in response to United Nations Security Council Resolutions concerning AML/CFT, including UNSCR 1373;
- any prior AML/CFT evaluations/assessments and/or self-assessment reports, and any other relevant report e.g. FSAP report on banking supervision;
- information on on-going or planned legislative or regulatory initiatives.

[5] All relevant laws, regulations and other documents should be provided in the original language and the language of the evaluation/assessment.

23. An important component of the information to be provided by examined countries are statistics. These are essential to allow assessors to assess the effectiveness of the implementation of the FATF 40+9 Recommendations and to deliver fair and accurate ratings. Countries should ensure that they provide data which is as complete and up to date as possible.

VI. Instructions for preparing the on-site visit

24. The MEQ is intended to aid the FATF Secretariat provide assessors with an outline of the MER prior to the on-site visit. This outline (a preliminarily draft report) will be based on the questionnaire responses (information on both the essential criteria and the additional elements). Any missing issues, incomplete responses or omissions will be noted. It will also reflect a first brief analysis of the AML/CFT system of the examined country. Assessors will need to carefully examine this outline and have a good overall understanding of the AML/CFT system of the examined country prior to the on-site visit. Their attention should essentially focus on any outstanding issues, weaknesses or other substantive points raised in the outline or discovered in the course of their own reading/analysis. Assessors should note the strengths and weaknesses of the system and be ready to question the national authorities and bodies to be met during the on-site visit. The MEQ should remain a document of reference, especially during the discussions at the time of the on-site visit.

25. During the on-site visit, examined countries should organise meetings with a range of government Ministries and agencies, as well as the private sector. In all AML/CFT evaluations/assessments missions, the following authorities and businesses should be visited:

Ministries:

- Ministry of Finance;
- Ministry of Justice, including central authorities for international co-operation;
- Ministry of Interior;
- Ministry of Foreign Affairs;
- Ministry responsible for the law relating to legal persons, legal arrangements and non-profit organisations;
- Other bodies or committees to co-ordinate AML/CFT action.

Criminal justice and operational agencies:

- The FIU;
- Law enforcement agencies including police and other relevant investigative bodies;
- Prosecution authorities including specialised confiscation agencies;
- Customs service;
- If relevant - specialised drug agencies, intelligence or security services, tax authorities;
- Task forces or commissions on ML, FT or organised crime.

Financial sector bodies:

- Ministries or agencies responsible for licensing, registering or otherwise authorising financial institutions;
- Supervisors of financial institutions, including the supervisors for banking and other credit institutions, insurance, and securities and investment;
- Supervisors or authorities responsible for monitoring and ensuring AML/CFT compliance by other types of financial institutions, in particular bureaux de change and money remittance businesses;
- Exchanges for securities, futures and other traded instruments;

- If relevant, Central Bank;
- The relevant financial sector associations, as well as a representative sample of financial institutions (this could include both senior executives and compliance officers, and where appropriate internal auditors);
- A representative sample of external auditors.

DNFBP and other matters:

- Casino supervisory body;
- Supervisor or other authority or SRO responsible for monitoring AML/CFT compliance by other DNFBP;
- Self-regulatory organisations (SRO) for professionals such as lawyers, notaries and accountants;
- Registry for companies and other legal persons, and for legal arrangements (if applicable);
- Bodies or mechanisms that oversight non-profit organisations, for example tax authorities (where relevant);
- Any other agencies or bodies that may be relevant;
- A representative sample of professionals involved in non-financial businesses and professions (managers or persons in charge of AML/CFT matters (e.g. compliance officers) in casinos, real estate agencies, precious metals/stones businesses as well as lawyers, notaries, accountants and any person providing trust and company services).

Efficient use has to be made of the time available on-site, and it is therefore suggested that the meetings with the financial sector and DNFBP associations also have the representative sample of institutions/DNFBP present.

VII. Instructions for preparing the mutual evaluation report

26. The MER should be prepared on the basis of the current FATF 40 + 9 Recommendations using the 2004 Methodology. FSRBs may also wish to add recognised regional AML/CFT standards e.g. the EU Money Laundering Directives, to the scope of their evaluations/assessments. Such standards should be consistent with the FATF Recommendations, in which case, any additional AML/CFT elements should be clearly identified and could be appropriately appended. The description of the system in place, the analysis and any recommendations should cover all the essential criteria. A typical MER would normally be expected to be not longer than 150 pages in length.

27. At the end of the on-site visit, assessors and the FATF Secretariat will meet to discuss all major issues and recommendations and agree on the ratings. These meetings on-site between the assessors and the Secretariat are essential to reach agreement on key issues and launch the drafting of the MER. Assessors will have two weeks after the on-site visit to provide written comments on their additional findings.

(a) Components of each part of Section 2-6 of the MER

"Description and Analysis"

28. The description section should be concise, while providing the authorities and any readers with sufficient information to support the subsequent analysis and compliance rating on the related FATF 40+9 Recommendations. It should always cover all the issues set out in the essential criteria, and should also address the additional elements. The degree to which the additional elements are discussed will vary from country to country. The description should comprehensively cover all the laws,

regulations or other measures that are relevant to the essential criteria, as well as any relevant statistical or other data. It may also cover other laws, regulations or measures that are relevant to the AML/CFT system (though not part of the essential criteria or additional elements), but such other aspects should be described succinctly. Descriptions should provide direct citations and/or concise quotes or summaries sufficient to accurately describe and source the relevant elements of the law, regulation or other applicable measure.

29. Assessors should analyse the laws, regulations and other measures and clearly identify any aspects of the AML/CFT system that are missing or which are insufficiently addressed. They should also verify and note whether the required measures have been properly and effectively implemented, and that the system is effective. In doing so they should have regard to appropriate statistics and other data, as well as any other information received in writing or as part of the on-site visit. Areas of weaknesses should be described as fully as needed to identify the measures needed to improve the AML/CFT system and its effectiveness, and to achieve compliance with the FATF Recommendations. Similarly, where aspects of the AML/CFT system are comprehensive and effective, this should be appropriately noted.

"Recommendations and Comments"

30. The assessor should provide appropriate recommendations addressing each of the areas of weakness that leads to a less than fully compliant rating. These recommendations form the basis for completing Table 2 Recommended Action Plan. Even where a country is fully compliant with particular FATF Recommendations, assessors should advise on areas which might be useful for enhancing the AML/CFT system.

"Compliance with FATF Recommendations"

31. Every Recommendation in the 40 + 9 Recommendations should be rated. Individual criterion should not be rated. There are four possible compliance ratings (compliant, largely compliant, partially compliant and non-compliant, see paragraph 11 of the 2004 Methodology), and exceptionally, a Recommendation could be rated as not applicable:

Compliant	The Recommendation is fully observed with respect to all essential criteria.
Largely compliant	There are only minor shortcomings, with a large majority of the essential criteria being fully met.
Partially compliant	The country has taken some substantive action and complies with some of the essential criteria.
Non-compliant	There are major shortcomings, with a large majority of the essential criteria not being met.
Not applicable	A requirement or part of a requirement does not apply, due to the structural, legal or institutional features of a country e.g. a particular type of financial institution does not exist in that country.

32. In determining the level of compliance for each Recommendation, the assessor should not only assess formal compliance with the FATF Recommendations, but will also assess compliance having regard to whether the Recommendations have been fully and properly implemented[6] and that this implementation is effective. This requires an assessment not only of whether the necessary implementing measures are in force and effect, but also whether the results obtained, e.g. the number of

[6] Full and proper implementation requires that all the necessary laws, regulations, guidelines etc are in force and effect, and that any necessary institutional framework is in place.

ML convictions or the number of STR filed, show that the system is effective. The issue of effectiveness is dealt with in the 2004 Methodology (see paragraphs 6, 7 and 15-18) and assessors should have regard to this. In making their assessment, assessors should note that the onus is on assessed countries to demonstrate (whether through statistics or by other factors) that its AML/CFT system meets the FATF Recommendations and is effective.

33. To assist assessors, a list of factors or elements that assessors could have regard to (as guidance only) when assessing whether the Recommendations have been effectively implemented is set out in Annex 3. This list of factors or elements is not to be regarded as exhaustive. Assessors will continue to have discretion to consider other effectiveness elements, or to disregard the listed elements if they are not applicable in the assessed country, having regard to the particular circumstances of an individual assessment. In the report, assessors should clearly state the basis on which they measured effectiveness, and the rationale for their conclusions and rating.

34. In order to ensure proper transparency, to help ensure consistency, and so that the country knows the basis for its rating, the section that sets out the compliance rating should also set out clearly, though in a very short point form, the factors that were taken into account in fixing that rating. This should state: (a) whether the essential criteria have been fully met, and if not, what aspects are deficient, (b) how the assessment of the effectiveness affected the rating. The effectiveness of the system in particular areas may have a positive, neutral or negative influence on the rating. As many of these elements will have already been stated in the analysis, the bullet points should only be very short and could refer to relevant paragraphs of the report. Some Recommendations are referred to in more than one section e.g. Recommendations 30 and 32. This does not mean that there should be partial ratings for each section. One rating should be recorded, but only the factors that affect that particular sub-section of the report should be recorded in the sub-section.

(b) Additional and other elements of the AML/CFT system

35. When preparing the MER, assessors should write up the additional elements in the 2004 Methodology, together with any other relevant elements of the country's AML/CFT system that are not expressly mentioned in the 2004 Methodology, in the section of the report to which they are linked or form part of. For example, additional element 1.8, which is integrally linked to essential criterion 1.5 should be written up in the part of the report that deals with criteria 1.5. However, the report must clearly delineate between the essential criteria and other non-mandatory aspects of the AML/CFT system.

(c) Laws, regulations and other measures to be in force and effect

In force and effect

36. In preparing the report and in giving ratings, assessors should only take into account relevant laws, regulations or other AML/CFT measures that 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. Where bills or other firm proposals to amend the system are made available prior to or at the time of the on-site visit, these may be referred to in the report (description, analysis and recommendations), but should not be taken into account for ratings purposes unless they are in force and effect in the period immediately following the on-site mission. While this period is not precisely fixed, it would not normally extend beyond a date two months after the on-site visit. Information relating to significant new AML/CFT initiatives after this period should only be referenced by footnote.

Law or regulation or other enforceable means

37. Certain essential criteria applicable to financial institutions and/or DNFBP in the 2004 Methodology are basic obligations and need to be set out in law or regulation, while the remainder

could be required by other enforceable means. The 2004 Methodology criteria in respect of Recommendations 5, 10 and 13 that are basic obligations are marked with an asterisk (*). More detailed elements in the criteria in respect of Recommendations 5, 10 and 13, as well as obligations under Recommendations 6-9, 11, 14-15, 18, and 21-22 could be required either by law or regulation or by other enforceable means.

38. *Law or regulation* means to primary and secondary legislation, such as laws, decrees, implementing regulations or other similar requirements, issued or authorised by a legislative body, and which impose mandatory requirements with sanctions for non-compliance. *Other enforceable means* refers to guidelines, instructions or other documents or mechanisms that set out enforceable requirements with sanctions for non-compliance, and which are issued by a competent authority (e.g. a financial supervisory authority) or an SRO. In both cases, the sanctions for non-compliance should be effective, proportionate and dissuasive (see R.17).

39. For both categories, assessors should keep in mind the fundamental requirements for any measure. It should:

a) impose a legal obligation;
b) the obligation should be legally enforceable either by criminal, civil or administrative means; and
c) there should be effective, proportionate and dissuasive sanctions for persons that fail to comply with the obligation.

40. On the other hand, assessors should consider certain types of documents or measures are not sufficient to meet the requirements to implement the FATF Recommendations. Examples of inadequate documents or measures are as follows:

a) Codes of conduct issued by private sector associations;
b) Non-binding guidance issued by a supervisory authority; (guidelines without obligation or sanction);
c) Voluntary behaviour of the private sector (e.g. voluntarily issued internal policies).

(d) Risk of money laundering or terrorist financing

41. As noted in paragraphs 20-21 of the 2004 Methodology, an important 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. Assessors should normally prepare the MER and assess compliance on the basis that all financial institutions should be required to meet all the essential criteria in Recommendations 5-11, 13-15, 18 and 21-22. However, a country may take risk into account, and may decide to limit the application of certain FATF Recommendations provided that either of the conditions set out in paragraph 17 of the 2004 Methodology are met. This should be done on a strictly limited and justified basis. Equally, in Recommendation 5, a country may permit its financial institutions to take risk into account in deciding the extent of the CDD measures they will take.

41. Section 3.1 of the MER is the part of the report where the general approach that a country has taken on the issue of risk should be described and analysed. A country will be required to clearly state in its response to the mutual evaluation questionnaire whether, how and on what basis it has taken risk into account. If a country has not taken certain measures, or has taken reduced measures, based on a proven low risk of money laundering or terrorist financing, then it will have to note this in its response to the mutual evaluation questionnaire, and set out the basis for the decision.

42. Assessors will need to review the approach that has been taken on risk. Assessors should be satisfied as to the adequacy of the process to determine that there is a low risk of money laundering or terrorist financing, and the reasonableness of the conclusions, including conclusions as to any exemptions or limitations that are to be allowed. Risk is relevant in the following areas:

a) Measures that countries require financial institutions to take under Recommendations 5-11, 13-15, 18 and 21-22. A country may decide not to apply some or all of the requirements under one or more of these Recommendations, provided that:

   (i) the relevant financial activity 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 (in addition to the issues raised above, assessors should also be satisfied that the relevant financial activity is carried out on an occasional or very limited basis); or

   (ii) there is a proven low risk of money laundering and terrorist financing, and that the exemptions or limitations are done on a strictly limited and justified basis.

b) Under Recommendation 5, a country may permit its financial institutions to take risk into account in deciding the extent of the CDD measures they will take (see criteria 5.8-5.12). Financial institutions may thus reduce or simplify (but not avoid completely) the required measures. 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.

c) Under Recommendation 23 (for financial institutions other than those subject to Core Principles), a country may have regard to the risk of money laundering or terrorist financing in a particular financial sector when determining the extent of measures to license or register and appropriately regulate, and to supervise or oversight for AML/CFT purposes. If there is a proven low risk of money laundering and terrorist financing then lesser measures may be taken.

d) Under Recommendation 15, a country may have regard to the risk of money laundering or terrorist financing, and to the size of the business, when determining the type and extent of measures required in that financial sector.

e) As regards DNFBP:

   (i) In applying Recommendation 5 to DNFBP, a country may permit DNFBP to take risk into account in deciding the extent of the CDD measures they will take having regard to the type of customer, product or transaction (see also criteria 5.8-5.12).

   (ii) Under Recommendation 24, a country may have regard to the risk of money laundering or terrorist financing in a particular DNFBP sector when determining the extent of measures required to monitor or ensure compliance for AML/CFT purposes. If there is a proven low risk of money laundering and terrorist financing then lesser measures may be taken.

f) As regards non-profit organisations (SR.VIII), a country may have regard to the risk of money laundering or terrorist financing for particular types of non-profit organizations, and take into account relevant issues such as the size of the organisation, the amount of funds it handles, and its specific objectives.

(e) Federal systems and supranational measures

43. 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. Examples include countries where the power to pass laws governing predicate offences for money laundering exist at both federal and state levels, or where a particular financial sector is supervised at the state level. Countries are requested in the mutual evaluation questionnaire to note the AML/CFT measures that are the responsibility of state/provincial/local level authorities, and to provide an appropriate description of these measures. Assessors should be aware that AML/CFT measures may be taken at one or more levels of government and examine all the measures that are necessary for combating money laundering and terrorist financing. Where measures are being taken at a state/provincial/local level, then these should be noted in the report and taken into account for ratings purposes.

44. Equally, assessors should take into account and refer to supranational laws or regulations that apply to a country. The clearest example may be where measures are taken within the European Union and apply directly to member states, such as EC Regulations.

(f) Sanctions

45. The essential criteria under Recommendation 17 set out a number of requirements relating to the need for effective, proportionate and dissuasive sanctions, where natural or legal persons do not comply with the AML/CFT requirements applicable to them. The sanctions applicable to financial institutions are considered under Recommendation 17, while sanctions for DNFBP are dealt with under Recommendation 24. These sanctions could be contained within specific provisions that are part of the laws or regulations that set out the requirement, or could be part of more general powers of sanction that are given to competent authorities to ensure that they can adequately enforce their supervisory or monitoring role. Where there are specific sanction provisions these should be noted in the sections of the report that deal with those requirements e.g. specific sanctions within AML laws for failure to report suspicious transactions should be dealt with in section 3.7. However more general powers of sanction that are given to competent authorities such as financial supervisory authorities should be noted in the sections that deal with those authorities and their powers e.g. section 3.10.

ANNEXES

Annex 1

MUTUAL EVALUATION/DETAILED ASSESSMENT QUESTIONNAIRE
ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

[*NAME OF COUNTRY*]

QUESTIONNAIRE TEMPLATE

[Date]

Introduction

i. This questionnaire is the means by which the authorities in the country[7] being evaluated can provide all the detailed input to the evaluation process prior to the on-site mission. This input should primarily describe the measures that are currently in place, including the implementation measures and the results obtained. Countries should also describe measures or changes which are not yet in place, but which they plan to implement – these measures should be clearly delineated from those that are in place at the time of the on-site visit. Finally, authorities may also set out any additional analysis or commentary that they believe would assist the assessors in carrying out the evaluation e.g. their analysis of the effectiveness of the measures in place.

ii. This standard questionnaire was agreed at the FATF Plenary meeting in June 2004 (and amended in June 2005 and February 2006), and copies were made available to all FATF members and observers, including all FATF-style regional bodies, the OGBS and the IMF and the World Bank. If a country does not have the questionnaire for FATF evaluations, it should be sent to the country for completion as soon as possible, and in any event, at least five (5) months prior to the on-site mission (where this is possible).

iii. The questionnaire should be comprehensively completed and returned at least two (2) months prior to the commencement of the on-site mission. It is essential that the material be provided by this date if the necessary preparatory work is to be done. The questionnaire response should be accompanied by copies of all relevant laws, regulations, guidelines and other material referenced in the response (both in the language of the country and the language of the evaluation). All documents should be supplied in the agreed language of the evaluation.

[7] All references to "country" also include territories or jurisdictions.

QUESTIONNAIRE FOR MUTUAL EVALUATIONS

The country being evaluated should provide responses for each section of the questionnaire in the manner set out below.

1. Section 1

1.1 General information on the country and its economy

1. In section 1.1, countries should provide general information on the country and the economy. Other information that could be relevant would be a short summary addressing the six structural elements referred to in paragraph 7 of the AML/CFT Methodology 2004, or notable deficiencies in pre-conditions for an effective AML/CFT framework. In certain countries it may also be relevant to include summarised information on the level of development of the jurisdiction and other factors that affect the development and implementation of an AML/CFT framework.

1.2 General Situation of Money Laundering and Financing of Terrorism

2. This section provides background information on the types of predicate offences that are generating illegal proceeds that are laundered (whether those offences are domestic or foreign), any estimates of the amount of money being laundered, and the methods, techniques and trends that have been observed regarding the laundering. Information should also be provided on any terrorist activity that has occurred within the country, and on the sources and methods used to finance terrorist activity. Any specific matters of concern or vulnerability should be highlighted. The following questions should be answered:

(a) What crimes or types of crime are considered to be the major sources of illegal proceeds in your jurisdiction? Please describe briefly the current situation and trends regarding such crimes e.g. how serious a money laundering problem they represent; any order of magnitude estimate you can provide of the scale of proceeds generated; whether the incidence of such crimes is increasing or declining, and whether the proceeds come from domestic or foreign predicate offences.

Please provide, if possible, available statistical data on the numbers of prosecutions and convictions for serious offences, by offence type, for the last four (4) years. This will help the assessors to have an overview of your crime situation generally. For offences that result in economic loss or damage please indicate (if figures are available) the total economic loss or damage resulting from these offences.

(b) Describe the present money laundering situation in your jurisdiction, and how it has changed (if at all) in the last four (4) years? What do you consider your most important money laundering problem? Do you anticipate any changes in the money laundering threat in the foreseeable future? In your description, please provide the following types of information:

a. the number of cases of money laundering or suspected money laundering;
b. the most common ways in which the money is laundered;
c. the types of financial institutions, DNFBP or other businesses used;
d. the types of groups involved in laundering operations;
e. whether the pattern of money laundering has changed following the introduction of anti-money laundering measures.)

(c) Describe the present terrorist financing situation in your country and how it has changed (if at all) in the last four (4) years? Do you anticipate any changes in the methods or techniques that will be used in the foreseeable future? In your description, cover any cases of actual or suspected terrorist financing which have come to light; the source of the funds (including whether legal or

illegal), the ways in which the funds were provided to the terrorists and how they were used, the types of institutions used, and the groups involved). Advise whether the terrorist financing techniques and trends have changed following the introduction of counter-terrorist financing measures.

1.3 Overview of the Financial Sector and DNFBP

3. Section 1.3 should contain a description of the types of financial institutions operating in the country, and listing the financial activities (see the definition of "financial institution" in the Methodology) that they engage in or are authorised to engage in. It is very useful if a table is prepared that compares the types of financial institutions operating in a country with the list of financial activities set out in the definition. For the purposes of the FATF Recommendations, it is not necessary that a business or institution requires authorisation to be classified as a "financial institution". Rather, this section should describe any natural or legal person that engages in a financial activity and meets the definition of "financial institution". The section should set out information on the number and size of financial institutions, and any recent changes of significance e.g. consolidation in a particular sector.

4. There should be similar information on each of the six categories of designated non-financial businesses and professions (DNFBP) as defined in the Forty Recommendations, namely: casinos (including internet casinos); real estate agents; dealers in precious metals; dealers in precious stones; lawyers, notaries, other independent legal professionals and accountants; and trust and company service providers. The section should describe the types of activities or business that they typically engage in, or are permitted to engage in, as well as information on the number and size of these various businesses and professionals (as defined), and any recent changes of significance.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements

5. This section should contain a description of the types of legal persons and legal arrangements that can be established or created, or can own property, in the country. This may extend to types of legal persons and arrangements that cannot be created within the country but which are recognised for purposes such as holding bank accounts or real estate, owning shares or conducting financial transactions. The country should provide basic information on:

(a) how such legal persons or arrangements are created or established or are otherwise recognised e.g. what formal documents are required;

(b) the basic characteristics of such entities e.g. who has ownership (for example shareholders, which could be legal or natural persons) and control (e.g. directors), do they require a registered office or agent etc.;

(c) whether they are registered, what types of information must be provided for the register (in particular, information on ownership and control), and whether this is public information; and

(d) what types of information concerning its ownership and control must be maintained by the entity itself, who has access to this information and must it be retained in the country where it is created or established or owns property.

It is very useful if this section also contains a description of any laws, systems and mechanisms that exist for identifying natural persons, which could be through national identity registration systems, use of identity cards or in other ways.

1.5 Overview of strategy to prevent money laundering and terrorist financing

6. This section should provide a high-level overview of the country's AML/CFT efforts, and in particular the policy objectives and any progress that has been made since the last evaluation. It not necessary to give an overview of the whole system, as all the legislative and other components are described in detail below, and the executive summary of the MER will provide this overview. It should include

identification of the authorities, bodies and institutions with AML/CFT responsibilities within the country and a summary of historical developments. The responses to the questions below will help to provide a substantial basis for completing this section.

a. AML/CFT Strategies and Priorities

i. What are the current control policies and objectives of your government for combating money laundering or terrorist financing? Describe which aspects of the anti-money laundering policies and/or programmes have the highest priority? Why?

ii. Have you measured the effectiveness of your policies and programmes? If so, describe how this was done, and what the results are.

iii. Describe any new initiatives that your government is planning for combating money laundering or terrorist financing?

b. The institutional framework for combating money laundering and terrorist financing

Describe briefly the roles and responsibilities of the various governmental and non-governmental authorities or organisations in detecting, preventing, and taking repressive action in relation to money laundering and terrorist financing, both at the national level and sub-national levels (e.g. state or provincial) if applicable, highlighting any recent changes. This also includes Ministries or bodies involved in setting AML/CFT policy. For example:

Ministries

- Ministry of Finance.
- Ministry of Justice, including central authorities for international co-operation.
- Ministry of Interior.
- Ministry of Foreign Affairs.
- Ministry responsible for the law relating to legal persons and arrangements.
- Committees or other bodies to co-ordinate AML/CFT action.

Criminal justice and operational agencies

- The financial intelligence unit (FIU).
- Law enforcement agencies including police and other relevant investigative bodies.
- Prosecution authorities including specialised confiscation agencies.
- Customs service.
- If relevant - specialised drug agencies, intelligence or security services, tax authorities.
- Task forces or commissions on ML, FT or organised crime.

Financial sector bodies

- Ministries or agencies responsible for licensing, registering or otherwise authorising financial institutions.
- Supervisors of financial institutions, including the supervisors for banking and other credit institutions, insurance, and securities and investment.
- Supervisors or authorities responsible for monitoring and ensuring AML/CFT compliance by other types of financial institutions, in particular bureaux de change and money remittance businesses.
- Exchanges for securities, futures and other traded instruments.
- Central Bank.

DNFBP and other matters

- Casino supervisory body.
- Supervisor or other competent authority, or SRO, for DNFBP.
- Self-regulatory organisations (SRO) for professionals such as lawyers and accountants.

- Registry for companies and other legal persons, and for legal arrangements (if applicable).
- Mechanisms relating to non-profit organisations.
- Any other agencies or bodies that may be relevant.

c. Overview of policies and procedures

Please provide an overview of any policies and procedures that your authorities have adopted in applying a risk-based approach to combating money laundering and terrorist financing. The overview should describe the authorities' overall philosophy towards a risk-based approach (e.g. does it form an integral part of its regulatory framework?), and should indicate how the relevant risk assessments are undertaken to help determine the policy and its practical application. Finally, there should be a description of the mechanism by which any permitted variations from the generally applicable standards are promulgated, and what arrangements, if any, are in place to monitor the continuing suitability of the exceptions.

d. Progress since the last mutual evaluation or assessment

Where a country has undergone a previous mutual evaluation or detailed assessment, the country should summarise the key findings and/or recommendations that were made in the previous report (a copy of which should be made available to assessors), and set out the measures that the country had taken to address the recommendations in the period up to the date of the on-site visit or immediately thereafter.

2. Sections 2 – 7

In each part of the sections below there is a table setting out all the criteria under the 2004 Methodology. Countries should complete the descriptive component as set out in the table. They may also out provide any additional analysis or commentary that they believe would assist the assessors in carrying out the evaluation.

Description and Analysis	A detailed description of the laws, regulations and other measures currently in place that are relevant to the section and to the Recommendation, including the implementation measures and the results obtained. Countries should also describe measures or changes which are not yet in place, but which are planned - these measures should be clearly delineated from those that are in place at the time of the on-site visit. The description must fully cover all essential criteria set out in the Methodology. Countries should also respond to the questions posed in the additional elements, though the level of detail may vary depending on the issue and the approach that a country has taken. For example, if a country has implemented one of the optional measures set out as an additional element, they should provide an adequate description of the measures taken. Any other relevant measures should also be adequately described. Descriptions should provide citations, quotes or summaries sufficient to describe the relevant elements of the law or other measures. To assist countries ensure that the description of their AML/CFT system covers all the essential criteria and additional elements, the criteria are set out in the questionnaire next to the relevant section of the report. Additional elements (which are not mandatory) and which will not be taken into account in the ratings appear in shaded boxes, as do the example boxes that are contained within the essential criteria. Where statistics are referred to in various parts of the questionnaire (R.32) countries should indicate not only whether they keep such statistics, but should provide the relevant statistics. Countries could also provide any other statistics or data that they consider to be relevant to the effectiveness and efficiency of their system for combating money laundering and terrorist financing. Authorities may (if they wish) indicate the extent to which they believe they have met the FATF Recommendations and may provide other comments or other supplementary information, such as their analysis of the effectiveness of the measures in place.

2 Legal System and Related Institutional Measures

Laws and Regulations

2.1 Criminalisation of Money Laundering (R.1 & 2)

2.1.1 Description and Analysis[8]

	Recommendations 1 & 2
General description of laws or other measures, the situation, or context.	
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.	
1.2.1 When proving that property is the proceeds of crime it should not be necessary that a person be convicted of a predicate offence[9].	
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.	

[8] Note to the assessed country and to the assessment team: for all Recommendations, the description and analysis section should include an analysis of effectiveness, and should contain any relevant statistical data.

[9] This criterion applies at any stage of the proceedings, including when a decision is being made whether to initiate proceedings.

1.4 Where countries apply a threshold approach or a combined approach that includes a threshold approach [10] , predicate offences should at a minimum comprise all offences: a) which 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.	
1.7 There should be appropriate ancillary offences to the offence of money laundering, including conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.	

[10] 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.

Additional elements 1.8 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, does this constitute a money laundering offence?	

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 Criminal liability for ML should extend to legal persons. Where that is not possible (i.e. due to fundamental principles of domestic law), civil or administrative liability should apply.	
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.	
	Recommendation 32 (money laundering investigation/prosecution data)
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: (b)(i) ML investigations, prosecutions, and convictions; If maintained, please provide these statistics	
Additional elements:	

32.3: Do competent authorities maintain comprehensive statistics on: (b) any criminal sanctions applied to persons convicted of ML offences?	
Please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

	Special Recommendation II
General description of laws or other measures, the situation, or context.	
II.1 Terrorist financing should be criminalised consistent with Article 2 of the Terrorist Financing Convention, and should have the following characteristics:[11] (a) Terrorist financing offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used, in full or in part: (i) to carry out a terrorist act(s); (ii) by a terrorist organisation; or (iii) by an individual terrorist. (b) Terrorist financing offences should extend to any *funds* as that term is defined in the TF Convention. This includes funds whether from a legitimate or illegitimate source. The Terrorist Financing Convention defines *funds* as: "assets of every kind, whether tangible or	

[11] Note to assessors: the criminalisation of terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy does not comply with SRII.

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." (c) Terrorist financing offences should not require that the funds: (i) were actually used to carry out or attempt a terrorist act(s); or (ii) be linked to a specific terrorist act(s). (d) It should also be an offence to attempt to commit the offence of terrorist financing. (e) It should also be an offence to engage in any of the types of conduct set out in Article 2(5) of the Terrorist Financing Convention.	
II.2 Terrorist financing offences should be predicate offences for money laundering.	
II.3 Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur	
II.4 Countries should ensure that Criteria 2.2 to 2.5 (in R.2) also apply in relation to the offence of FT.	
	Recommendation 32 (terrorist financing investigation/prosecution data)
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: (b)(i) FT investigations, prosecutions, and convictions;	
<u>Additional elements:</u> 32.3: Do competent	

authorities maintain comprehensive statistics on: (b) any criminal sanctions applied to persons convicted of FT offences? If maintained, please provide these statistics	
If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)

2.3.1 Description and Analysis

	Recommendation 3
General description of laws or other measures, the situation, or context.	
3.1 Laws should provide for the confiscation of property that has been laundered or which constitutes: a) proceeds from; b) instrumentalities used in; and c) instrumentalities intended for use in the commission of any ML, FT or other predicate offences, and property of corresponding value.	
3.1.1 Criterion 3.1 should equally apply: (a) to property that is derived directly or indirectly from proceeds of crime; including income, profits or other benefits from the proceeds of crime; and (b) subject to criterion 3.5, to all the property referred to above, regardless of whether it is held or owned by a criminal defendant or by a third party. All the property referred to in criteria 3.1 and 3.1.1 above is hereafter referred to as "property subject to confiscation".	
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 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.	
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.	
<u>Additional elements</u> 3.7 Do laws 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)? 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?	
	Recommendation 32 (confiscation/freezing data)

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: …… (b)(ii) The number of cases and the amounts of property frozen, seized, and confiscated relating to (i) ML, (ii) FT, and (iii) criminal proceeds;	
Additional elements: 32.3: Do competent authorities maintain comprehensive statistics on: (d) the number of cases and the amounts of property frozen, seized, and confiscated relating to underlying predicate offences where applicable? If maintained, please provide these statistics	
If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and Analysis

	Special Recommendation III
General description of laws or other measures, the situation, or context.	
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). Such freezing should take place without delay and without prior notice to the designated persons involved. S/RES/1267(1999) and its successor resolutions 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.	
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). Such freezing should take place without delay and without prior notice to the designated persons involved. S/RES/1373(2001) obligates countries 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 country 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 countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries. When (i) a specific notification or communication is sent and (ii) the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organisation, the country receiving the request must ensure that the funds or other assets of the designated person are frozen without delay.	
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, according to applicable national legal principles, whether reasonable grounds or a reasonable basis exists to initiate a freezing action and the subsequent freezing of funds or other assets without delay.	
III.4 The freezing actions referred to in Criteria III.1 – III.3 should extend to: a) funds or other assets wholly or jointly[12] 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	

[12] *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.

designated persons, terrorists, those who finance terrorism or terrorist organisations.	
III.5 Countries should have effective systems for communicating actions taken under the freezing mechanisms referred to in Criteria III.1 – III.3 to the financial sector [13] immediately upon taking such action.	
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	

[13] For examples of possible mechanisms to communicate actions taken or to be taken to the financial sector and/or the general public, see the FATF Best Practices paper entitled "Freezing of Terrorist Assets – International Best Practices".

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, administrative or criminal sanctions for failure to comply with such legislation, rules or regulations.	
Additional elements III.14 Have the measures set out in the Best Practices Paper for SR.III been implemented? III.15 Have the 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 been implemented? Are these procedures consistent with S/RES/1373(2001) and the spirit of S/RES/1452(2003)?	
	Recommendation 32 (terrorist financing freezing data)
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: (iii) Number of persons or entities and the amounts of property frozen pursuant to or under U.N. Resolutions relating to terrorist financing. If maintained, please provide these statistics	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

Authorities

2.5 The Financial Intelligence Unit and its functions (R.26, 30 & 32)

2.5.1 Description and Analysis

	Recommendation 26
General description of laws or other measures, the situation, or context.	
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 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 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 publicly release periodic reports, and such reports should include statistics, typologies and trends as well as information regarding its activities.	
26.9 Where a country has created an FIU, it should consider applying for membership in the Egmont Group.	
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 30 (FIU):
30.1 FIU only: 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 influence or interference.[14]	
30.2 FIU only: 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 FIU only: Staff of competent authorities should be provided with adequate and relevant training for combating ML and FT. Examples of issues to be covered under adequate and relevant training include: 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; the use of information technology and other resources relevant to the execution of their functions. Countries could also provide special training and/or certification for financial investigators for, *inter alia*,	

[14] If a country's FIU does not comply with the requirement to have sufficient operational independence and autonomy (Criterion 26.6), the country should only be rated down in Recommendation 26.

investigations of ML, FT, and the predicate offences.	
	Recommendation 32 (FIU):
32.2 FIU: 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 – (i) STR received by the FIU, including a breakdown of the type of financial institution, DNFBP, or other business or person making the STR; (ii) Breakdown of STR analysed and disseminated; (iii) international wire transfers (It is acceptable if these statistics are kept by another agency). If maintained, please provide these statistics	
<u>Additional elements:</u> 32.3 FIU only (It is acceptable if this information is kept by other agencies): Do competent authorities maintain comprehensive statistics on: (a) STR resulting in investigation, prosecution, or convictions for ML, FT or an underlying predicate offence?	
If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27, 28, 30 & 32)

2.6.1 Description and Analysis

	Recommendation 27
General description of laws or other measures, the situation, or context.	
27.1 There should be designated law enforcement [15] authorities that have responsibility for ensuring that ML and FT offences are properly investigated.	
27.2 Countries should consider taking measures, whether legislative or otherwise, that allow competent authorities investigating ML cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering.	
<u>Additional elements:</u> 27.3 Are measures in place, whether legislative or otherwise, that provide law enforcement or prosecution authorities with an adequate legal basis for the use of a wide range of special investigative techniques when conducting investigations of ML or FT (e.g. controlled delivery of the proceeds of crime or funds intended for use in terrorism, undercover operations, etc)? 27.4 Where special investigative techniques are permitted, are such techniques used when conducting investigations of ML, FT, and underlying predicate offences, and to what extent? 27.5 In addition to special investigative techniques, are the following effective	

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

mechanisms used? (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? 27.6 Are ML and FT methods, techniques and trends reviewed by law enforcement authorities, the FIU and other competent authorities (as appropriate) on a regular, interagency basis? Are the resulting information, analyses or studies disseminated to law enforcement and FIU staff, as well as staff of other competent authorities?	
	Recommendation 28
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 30 (Law enforcement and prosecution authorities only)
30.1 Law enforcement & prosecution only: 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 influence or interference.	
30.2 Law enforcement: 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 Law enforcement: Staff of competent authorities should be provided with adequate and relevant training for combating ML and FT. Examples of issues to be covered under adequate and relevant training include: 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; the use of information technology and other resources relevant to the execution of their functions. Countries could also provide special training and/or certification for financial investigators for, *inter alia*, investigations of ML, FT, and the predicate offences.	
Additional elements 30.4 Are special training or educational programmes provided 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?	
Additonal material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis[16]

	Special Recommendation IX
General description of laws or other measures, the situation, or context.	
IX.1 To detect the physical cross-border transportation of currency and bearer negotiable instruments that are related to money laundering or terrorist financing, a country should implement one of the following two systems on incoming and outgoing[17] cross-border	

[16] The description of the system for reporting suspicious transactions in s.3.7 is integrally linked with the description of the FIU in s.2.5, and the two texts need to be complementary and not duplicative.

[17] Countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments.

transportations of currency or bearer negotiable instruments: (a) A declaration system that has the following characteristics: (i) All persons making a physical cross-border transportation of currency or bearer negotiable instruments that are of a value exceeding a prescribed threshold should be required to submit a truthful declaration to the designated competent authorities; and (ii) The prescribed threshold cannot exceed EUR/USD 15,000[18] OR (b) A disclosure system that has the following characteristics: (i) All persons making a physical cross-border transportation of currency or bearer negotiable instruments should be required to make a truthful disclosure to the designated competent authorities upon request; and (ii) The designated competent authorities should have the authority to make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.	
IX.2 Upon discovery of a false declaration/ disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or bearer negotiable instruments and their intended use.	

[18] Countries that implement a declaration system should ensure that the prescribed threshold is sufficiently low to meet the objectives of Special Recommendation IX. In any event, the threshold cannot exceed EUR/USD 15,000.

IX.3 The designated competent authorities should be able to stop or restrain currency or bearer negotiable instruments for a reasonable time in order to ascertain whether evidence of money laundering or terrorist financing may be found: (a) Where there is a suspicion of money laundering or terrorist financing; or (b) Where there is a false declaration/disclosure.	
IX.4 At a minimum, the amount of currency or bearer negotiable instruments declared/disclosed or otherwise detected, and the identification data of the bearer(s) shall be retained for use by the appropriate authorities in instances when: (a) A declaration which exceeds the prescribed threshold is made; or (b) Where there is a false declaration/disclosure; or (c) Where there is a suspicion of money laundering or terrorist financing.	
IX.5 The information obtained through the processes implemented in Criterion IX.1 should be available to the financial intelligence unit (FIU) either through: A system whereby the FIU is notified about suspicious cross-border transportation incidents; or By making the declaration/disclosure information directly available to the FIU in some other way.	
IX.6 At the domestic level, there should be adequate co-ordination among customs, immigration and other related authorities on issues related to the implementation of Special	

Recommendation IX.	
IX.7 At the international level, countries should allow for the greatest possible measure of co-operation and assistance amongst competent authorities, consistent with the obligations under Recommendations 35 to 40 and Special Recommendation V. Examples of possible measures (drawn from the Best Practices Paper to Special Recommendation IX) include: • Having co-operation arrangements with other countries which would allow for bilateral customs-to-customs information exchanges between customs and other relevant agencies on cross-border transportation reports and cash seizures. • Ensuring that the information recorded pursuant to criterion IX.4 can be shared internationally with foreign competent authorities in appropriate cases.	
IX.8 Countries should ensure that Criteria 17.1 to 17.4 (in R.17) also apply to persons who make a false declaration or disclosure contrary to the obligations under SR IX.	
IX.9 Countries should ensure that Criteria 17.1 to 17.4 (in R.17) also apply to persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering contrary to the obligations under SR IX.	
IX.10 Countries should ensure that Criteria 3.1 to 3.6 (in R.3) also apply in relation to persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to	

terrorist financing or money laundering.	
IX.11 Countries should ensure that Criteria III.1 to III.10 (in SR.III) also apply in relation to persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing.	
IX.12 If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should co-operate with a view toward establishing the source, destination, and purpose of the movement of such items and toward the taking of appropriate action.	
IX.13 Are the systems for reporting cross border transactions subject to strict safeguards to ensure proper use of the information or data that is reported or recorded?	
Additional elements **IX.14 Has the country implemented the measures in the Best Practices Paper for SR.IX?**	
IX.15 Where systems for reporting the cross border transportation of currency are in place, are the reports maintained in a computerised data base, available to competent authorities for AML/CFT purposes?	
	Recommendation 30 (Customs authorities[19]):
30.1 Customs authorities only: FIUs, law enforcement and	

[19] Other competent authorities could include bodies dealing with international co-operation such as a Central Authority, or Customs authorities (in some jurisdictions), or policy ministries.

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 influence or interference.[20]	
30.2 Customs authorities only: 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 Customs authorities only: Staff of competent authorities should be provided with adequate and relevant training for combating ML and FT. Examples of issues to be covered under adequate and relevant training include: 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; the use of information technology and other resources relevant to the execution of their functions. Countries could also provide special training and/or certification for financial investigators for, *inter alia*, investigations of ML, FT, and the predicate offences.	

[20] If a country's FIU does not comply with the requirement to have sufficient operational independence and autonomy (Criterion 26.6), the country should only be rated down in Recommendation 26.

	Recommendation 32
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 - (iii) Reports filed on: …… (ii) cross border transportation of currency and bearer negotiable instruments. If maintained, please provide these statistics	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

3. Preventive Measures - Financial Institutions

Please give a concise overview of the scope of coverage of AML/CFT preventive measures as they apply to the financial sector i.e. what sectors are covered and to what extent.

Description	

Customer Due Diligence & Record Keeping

3.1 Risk of money laundering or terrorist financing

A country may decide not to apply certain AML/CFT requirements, or to reduce or simplify the measures being taken, on the basis that there is a low or little risk of money laundering or terrorist financing. Similarly, as set out in R.5, financial institutions may, in certain circumstances determine the degree of risk attached to particular types of customers, business relationships, transactions or products. In section 3.1 countries should set out the basis upon which they have taken a decision not to apply certain required AML/CFT measures to a particular financial sector. Where there are specific references to risk in individual Recommendations (see Instructions to Assessors) the issue of risk for those Recommendations should be described in the relevant section of the MER i.e. sections 3.2, 3.8, 3.13 and 4.1, 4.4 and 4.5. See AML/CFT Methodology 2004, paragraphs 17-18.

Description	

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)

3.2.1 Description and Analysis

	Recommendation 5
General description of laws or other measures, the situation, or context.	
5.1* Financial institutions should not be permitted to keep anonymous accounts or accounts in fictitious names. 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[21] 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 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[22] 5.3* Financial institutions should be required to identify the customer (whether permanent or occasional, and whether natural or legal persons or legal arrangements) and verify that customer's identity using reliable, independent source documents, data or information (identification data)[23].	
5.4 For customers that are legal persons or legal arrangements, the financial institution should be required to: (a) * verify that any person	

[21] Financial institutions do not have to repeatedly perform identification and verification every time that a customer conducts a transaction.
[22] 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.
[23] 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.

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 of establishment or existence, and obtain information concerning the customer's name, the names of trustees (for trusts), legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement.	
5.5* Financial institutions should be required to identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner [24] using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is.	
5.5.1* 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.	
5.5.2 For customers that are legal persons or legal arrangements, the financial institution should be required to take reasonable measures to: (a) 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	

[24] For life and other investment linked insurance, the beneficiary under the policy must also be identified and verified. See criteria 5.14 concerning the timing of such measures.

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. Note to assessors: 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 shareholders of that public company.	
5.6 Financial institutions should be required to obtain information on the purpose and intended nature of the business relationship.	
5.7* Financial institutions should be required to conduct ongoing due diligence on the business relationship.	
5.7.1 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.	
5.7.2 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 reviews of existing records, particularly for higher risk categories of customers or business relationships.	
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 Basel CDD Paper) may include[25] 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 Where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures. 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[26] could include: a) Financial institutions – provided that they are	

[25] Other examples of higher risk are included in Recommendations 6 and 7.

[26] 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.

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. 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, this should be limited to countries that the original country is satisfied are in compliance with and have effectively implemented the FATF Recommendations.	
5.11 Simplified CDD measures are not acceptable whenever there is suspicion of money	

laundering or terrorist financing or specific higher risk scenarios apply.	
5.12 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.	
Timing of verification 5.13 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.	
5.14 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. c) The money laundering risks are effectively managed. Examples of situations where it may be essential not to interrupt the normal conduct of business 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.	
5.14.1 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 5.15 Where the financial institution is unable to comply with Criteria 5.3 to 5.5 above: a) it should not be permitted to open the account, commence business relations or perform the transaction; b) it should consider making a suspicious transaction report.	
5.16 Where the financial institution has already commenced the business relationship e.g. when Criteria 5.2(e), 5.14 or 5.17 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 and to consider making a suspicious transaction report.	
Existing customers 5.17 Financial institutions should be required to apply CDD requirements to existing customers[27] on the basis of materiality and risk and to conduct due	

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

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.	
5.18 Financial institutions should be required to perform CDD measures on existing customers if they are customers to whom Criterion 5.1 applies.	
	Recommendation 6
General description of laws or other measures, the situation, or context.	
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 Financial institutions should be required to obtain senior management	

approval for establishing business relationships with a PEP.	
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 elements 6.5 Are the requirements of R.6 extended to PEPS who hold prominent public functions domestically? 6.6 Has the 2003 United Nations Convention against Corruption been signed, ratified, and fully implemented?	
	Recommendation 7
General description of laws or other measures, the situation, or context.	
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 [28] 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.	
	Recommendation 8
General description of laws or other measures, the situation, or context.	
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	

[28] 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.

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.	
Additional Material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis

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[29]; (b) business relationships, accounts or transactions between financial institutions for their clients. These are addressed by R.5 and R.7.	***Recommendation 9***
General description of laws or other measures, the situation, or context.	
If financial institutions are permitted to rely on intermediaries or other third parties to perform some of the elements of the CDD process (Criteria 5.3 to 5.6)[30] 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 [31] concerning certain elements of the CDD process (Criteria 5.3 to 5.6).	
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 (in accordance with Recommendation 23, 24 and 29), 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	

[29] 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.
[30] 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.
[31] It is not necessary to obtain copies of documentation.

the FATF Recommendations[32].	
9.5 The ultimate responsibility for customer identification and verification should remain with the financial institution relying on the third party.	
Additional Material If you wish please indicate any other material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

	Recommendation 4
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.	
Additional Material If you wish please indicate any other material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

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

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis

	Recommendation 10
10.1* Financial institutions should be required to maintain all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction (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.	
SR VII applies to cross-border and domestic transfers between financial institutions. However, 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, such as withdrawals from a bank account through an ATM machine, cash advances from a credit card, or payments for goods and services. 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.	***Special Recommendation VII***
VII. For all wire transfers of EUR/USD 1 000 or more, ordering financial institutions should be required to obtain and maintain [33] the following information relating to the originator of 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). (This set of information is referred to as full originator information). For all wire transfers of EUR/USD 1 000 or more, ordering financial institutions should be	

[33] Financial institutions do not have to repeatedly obtain originator information and verify originator identity every time a customer makes a wire transfer. Financial institutions could rely on the information already available if, as part of the customer due diligence process, they have obtained:

(i) the originator's name;

(ii) account number (or unique reference number if no account number exists); and

(iii) address (or national identity number, customer identification number, or date and place of birth if the country permits one of these pieces of information to substitute for the address)

and verified the originator's identity in accordance with Recommendation 5 (see, in particular, criterion 5.3). This does not apply to occasional customers.

required to verify the identity of the originator in accordance with Recommendation 5.	
VII.2 For cross-border wire transfers of EUR/USD 1 000 or more the ordering financial institution should be required to include full originator information in the message or payment form accompanying the wire transfer. However, if several individual cross-border wire transfers (of EUR/USD 1 000 or more) from a single originator are bundled in a batch file for transmission to beneficiaries in another country, the ordering financial institution only needs to include the originator's account number or unique identifier on each individual cross-border wire transfer, provided that the batch file (in which the individual transfers are batched) contains full originator information that is fully traceable within the recipient country.	
VII.3 For domestic wire transfers the ordering financial institution should be required to either: (a) comply with Criterion VII.2 above or (b) include only the originator's account number or a unique identifier, within the message or payment form. The second option should be permitted only if full originator information can be made available to the beneficiary financial institution and to appropriate authorities within three business days of receiving a request, and domestic law enforcement authorities can compel immediate production of it.	
VII.4 Each intermediary and beneficiary financial institution in the payment chain should be required to ensure that all originator information that accompanies a wire transfer is transmitted with the transfer.	
VII.4.1. Where technical limitations prevent the full originator information	

accompanying a cross-border wire transfer from being transmitted with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution	
VII.5 Beneficiary financial institutions should be required to adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the financial intelligence unit or other competent authorities. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet SR.VII standards.	
VII.6 Countries should have measures in place to effectively monitor the compliance of financial institutions with rules and regulations implementing SR.VII..	
VII.7 Countries should ensure that Criteria 17.1 – 17.4 (in R.17) also apply in relation to the obligations under SR.VII.	
Additional elements VII.8 Countries may require that all incoming cross-border wire transfers (including those below EUR/USD 1 000) contain full and accurate originator information VII.9 Countries may require that all outgoing cross-border wire transfers below EUR/USD 1 000 contain full and accurate originator information .	

Additional Material If you wish please indicate any other material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

Unusual, Suspicious and other Transactions

3.6 Monitoring of transactions and relationships (R.11 & 21)

3.6.1 Description and Analysis

	Recommendation 11
General description of laws or other measures, the situation, or context.	
11.1 Financial institutions should be required to pay special attention to all complex, unusual large transactions, 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.	
	Recommendation 21
General description of laws or other measures, the situation, or context.	

21.1 Financial institutions should be required to give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply 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 countries	

applying the countermeasure 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.	
Additional Material If you wish please indicate any other material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

3.7 Suspicious transaction and other reporting (R.13-14, 19, 25 & SR.IV)

3.7.1 Description and Analysis[34]

	Recommendation 13& Special Recommendation IV
General description of laws or other measures, the situation, or context.	
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 [35] that funds are the proceeds 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	

[34] The description of the system for reporting suspicious transactions in s.3.7 is integrally linked with the description of the FIU in s.2.5, and the two texts need to be complementary and not duplicative.

[35] 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.

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 elements 13.5 Are financial institutions required 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 domestically?	
IV.1 A financial institution should be required by law or regulation to report to the FIU (a suspicious [36] transaction report – STR) when it suspects or has reasonable grounds to suspect that funds 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	

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

possible prosecution for a FT offence or otherwise (so called "indirect reporting"), is not acceptable.[37]	
IV.2 Countries should ensure that Criteria 13.3 – 13.4 (in R.13) also apply in relation to the obligations under SR IV.	
	Recommendation 14
General description of laws or other measures, the situation, or context.	
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 elements 14.3 Do laws or regulations or any other measures ensure that the names and personal details of staff of financial institutions that make a STR are kept confidential by the FIU?	
	Recommendation 25 (only feedback and guidance related to STRs)
General description of laws or other measures, the situation, or context.	

[37] Note to country being assessed: Do not duplicate text that is already set out under R.13 above. If need be cross-refer to the relevant text.

25.2 Competent authorities, and particularly the FIU, should provide financial institutions and DNFBP 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) may 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) subject to domestic legal principles, 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.	
	Recommendation 19
General description of laws or other measures, the situation, or context.	
19.1 Countries should consider the feasibility and utility of implementing a system where financial institutions report all transactions in currency above a fixed threshold to a national central agency with a computerised data base.	
<u>Additional elements</u> 19.2 Where systems for reporting large currency	

transactions are in place, are the reports maintained in a computerised data base, available to competent authorities for AML/CFT purposes? 19.3 Are the systems for reporting large currency transactions subject to strict safeguards to ensure proper use of the information or data that is reported or recorded?	
	Recommendation 32
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 - (iii) Reports filed on: (i) domestic or foreign currency transactions above a certain threshold, If maintained, please provide these statistics	
Additional Material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)

3.8.1 Description and Analysis

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.	***Recommendation 15***
General description of laws or other measures,	

the situation, or context.	
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.	
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 elements 15.5 Is the AML/CFT compliance officer able to act independently and to report to senior management above the compliance officer's next reporting level or the board of directors?	
	Recommendation 22
General description of laws or other measures, the situation, or context.	
22.1 Financial institutions should be required to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements and the FATF Recommendations, to the extent that local (i.e. host country) 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.	
22.1.2 Where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries should be required to apply the higher standard, to the extent that local (i.e. host country) laws and regulations permit.	
22.2 Financial institutions should be required to inform their home country supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (i.e. host country) laws, regulations or other measures.	
Additional elements 22.3 Are financial institutions subject to the	

Core Principles required to apply consistent CDD measures at the group level, taking into account the activity of the customer with the various branches and majority owned subsidiaries worldwide?	
Additional Material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

3.9 Shell banks (R.18)

3.9.1 Description and Analysis

	Recommendation 18
General description of laws or other measures, the situation, or context.	
18.1 Countries should not approve the establishment or accept the continued operation of shell banks.	
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.	
Additional Material If you wish please indicate any other material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

Regulation, supervision, guidance, monitoring and sanctions

3.10 Supervision and oversight

Note to countries - in completing this section of the questionnaire, countries should seek to address the various elements of the regulatory system and the relevant Recommendations, in the following sequence:

1. Describe all the competent authorities and SROs, and their roles, functions and duties in regulating the application of AML/CFT measures in the financial system, as well as describing their organisational structures and resources (R.23, R.30 - in particular criteria 23.1, 23.2, 30.1-30.3).
2. Set out the relevant powers (including sanction powers) of each authority and any other sanctions that are applicable for breaches of AML/CFT requirements (R.29, R.17 - all criteria).
3. Describe how market entry is regulated and how the authorities check the ownership/control of financial institutions regarding criminal records and where appropriate, fitness and properness (R.23 - in particular criteria 23.3, 23.3.1, 23.5 & 23.7 (licensing/registration elements only)).
4. Describe the process of ongoing supervision and monitoring, and include any available statistics regarding on-site or off-site inspections (R.23, R.32 - in particular criteria 23.4, 23.6, 23.7 (supervision/oversight elements only), 32.2d)
5. Explain any AML/CFT guidance/guidelines that have been provided by competent authorities to financial institutions (R.25 - criteria 25.1 only).

3.10.1 Description and Analysis

Note to assessors: Assessors should use criterion 23.1 to assess the overall adequacy of the regulatory and supervisory system, and to note any deficiencies that are not dealt with in other criteria. Assessors may also wish to have regard to matters raised in assessments made with respect to the Core Principles.	***Recommendation 23, 30, 29, 17, 32, & 25***
	Authorities/SROs roles and duties & Structure and resources - R.23, 30
General description of laws or other measures, the situation, or context.	
23.1 Countries should ensure that financial institutions are subject to adequate AML/CFT 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.	
R.30	***Resources (Supervisors)***
General description of laws or other measures, the situation, or context.	
30.1 Supervisors only: 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 influence or interference.	
30.2 Supervisors only: 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 Supervisors only: Staff of competent authorities should be provided with adequate and relevant training for combating ML and FT. Examples of issues to be covered under adequate and relevant training include: 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; the use of information technology and other resources	

relevant to the execution of their functions. Countries could also provide special training and/or certification for financial investigators for, inter alia, investigations of ML, FT, and the predicate offences.	
	Authorities Powers and Sanctions – R.29 & 17
General description of laws or other measures, the situation, or context.	
29.1 Supervisors should have adequate powers to monitor and ensure compliance by financial institutions [38] , with requirements to combat money laundering and terrorist financing, consistent with the FATF Recommendations.	
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.	
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	

[38] Note to assessors: With respect to foreign branches and subsidiaries, the requirement for financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures is to be assessed only against R.22. However, under R.29, supervisors should have adequate powers to establish that financial institutions require their foreign branches and majority owned subsidiaries to apply R.22 effectively.

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.	
R.17	
General description of laws or other measures, the situation, or context.	
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 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. 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. 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), 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, or criminal penalties where permitted.	
	Markey entry – R.23
General description of laws or other measures, the situation, or context.	
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.	
23.5 Natural and legal persons providing a money or value transfer service, or a money or currency changing service should be licensed or registered.	
23.7 Financial institutions (other than those mentioned in Criterion 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.	

[Focus only on the licensing/registration components of this criteria]	
	Ongoing supervision and monitoring – R.23 & 32
23.4 For financial institutions that are subject to the Core Principles [39] 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 and (iv) global consolidated supervision where required by the Core Principles.	
23.6 Natural and legal persons providing a money or value transfer service, or a money or currency changing service 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 Criterion 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	

[39] 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.

measures may be less. [Focus only on the supervision/oversight components of this criteria]	
R.32	
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: (d) Other action o On-site examinations conducted by supervisors relating to or including AML/CFT and any sanctions applied. If maintained, please provide these statistics	
	Guidelines – R.25 (Guidance for financial institutions other than on STRs)
General description of laws or other measures, the situation, or context.	
25.1 Competent authorities should establish guidelines that will assist financial institutions and DNFBP to implement and comply with their respective AML/CFT requirements. For DNFBP, such guidelines may be established by SROs. At a minimum, the guidelines should give assistance on issues covered under the relevant FATF Recommendations, including: (i) a description of ML and FT techniques and methods; and (ii) any additional measures that these institutions and DNFBP could take to ensure that their AML/CFT measures are effective.	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and	

efficiency of this part of the AML/CFT system.	

3.11 Money or value transfer services (SR.VI)

This section should very briefly summarise and cross-reference the description and any comments that have been made elsewhere in section 3 on money or value transfer services.

3.11.1 Description and Analysis (summary)

	Special Recommendation VI
General description of laws or other measures, the situation, or context.	
VI.1 Countries should designate one or more competent authorities 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[40].	
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 Nine Special Recommendations (in particular SR.VII).	
VI.3 Countries should have systems in place for monitoring 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 which must be made available to the designated competent	

[40] 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 Nine Special Recommendations.

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 elements VI.6 Have the measures set out in the Best Practices Paper for SR.VI been implemented?	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

4. Preventive Measures – Designated Non-Financial Businesses and Professions

Please give a concise overview of the scope of coverage of AML/CFT preventive measures as they apply to DNFBPs i.e. what sectors are covered and to what extent.

Description	

4.1 Customer due diligence and record-keeping (R.12)

(applying R.5, 6, 8-11 & 17 (only sanctions for these Recommendations))

Note to countries - in completing this section of the questionnaire, countries should seek to address the various elements of customer due diligence, record-keeping and monitoring and the relevant Recommendations, in the following sequence:

1. Describe the customer due diligence requirements and measures for DNFBP (applying R.5, 6, 8 & 9). Where requirements have already been described in Section 3 of the MEQ, it is only necessary to cross reference that material and to note any changes or differences of approach that may apply to DNFBP.
2. Set out the record-keeping requirements for DNFBP (applying R.10). Again this may be done in whole or part by cross-referencing.
3. Indicate if there are any differences for DNFBP regarding monitoring (applying R.11).
4. Set out the relevant sanctions that are applicable for breaches of the AML/CFT requirements under R.5, 6, & 8-11 (applying R.17). These should be sanctions applicable to all entities subject to the CDD and other requirements as opposed to sanction powers that are specific to the competent authorities or SROs which should be described in section 4.3 below. Again, it may be sufficient to cross-reference the material in Section 3 above.

4.1.1 Description and Analysis

	Recommendation 12
General description of laws or other measures, the situation, or context.	
12.1 DNFBP should be required to comply with the requirements set out in Recommendation 5 (Criteria 5.1 – 5.18) in the following circumstances[41]: a) Casinos (including internet casinos[42]) – when	

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

[42] Countries should establish rules to determine the basis upon which internet casinos are subject to national AML/CFT requirements. This will require the country to determine the basis or set or factors upon which it will decide whether there is a sufficient nexus or connection between the internet casino and the country. Examples of such factors include incorporation or organisation under the laws of the country, or place of effective management within the country. Assessors should examine the basis for the nexus or connection, with respect to R.12, 16 and 24.

their customers engage in financial transactions equal to or above USD/€ 3,000[43]. Examples of financial transactions in casinos include: the purchase or cashing in of casinos chips or tokens, the opening of accounts, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that involve only casino chips or tokens. b) Real estate agents – when they are involved in transactions for a client concerning the buying and selling of real estate[44]. 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[33]. 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 [45]; •management of bank, savings or securities accounts[30]; •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	

[43] 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.

[44] This means that real estate agents should comply with R.5 with respect to both the purchasers and the vendors of the property.

[45] 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.

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. DNFBP should especially comply with the CDD measures set out in Criteria 5.3 to 5.7 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 Criterion 12.1, DNFBP should be required to comply with the criteria set out under Recommendations 6 and 8-11.	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

4.2 Monitoring transactions and other issues (R.16)

(applying R.13-15, 17 & 21)

Note to countries - in completing this section of the questionnaire, countries should seek to address the various elements of monitoring and reporting system and the relevant Recommendations, in the following sequence:

1. Describe the suspicious transaction reporting system for DNFBP (applying R.13-14). Where the reporting obligations have already been fully described in Section 3 of the MEQ, it is only necessary to cross reference that material and to note any changes or differences of approach that may apply to DNFBP.
2. Set out the internal control requirements for DNFBP (applying R.15). Again this may be done in whole or part by cross-referencing.
3. Indicate if there are any differences for DNFBP regarding the application of R.21.
4. Set out the relevant sanctions that are applicable for breaches of the AML/CFT requirements under R.13-15 & 21 (applying R.17). These should be sanctions applicable

to all entities subject to reporting requirements as opposed to specific sanction powers of competent authorities or SROs which should be described in section 4.3 below. As such it may be sufficient to cross-reference the material in Section 3 above.

4.2.1 Description and Analysis

	Recommendation 16
General description of laws or other measures, the situation, or context.	
16.1 DNFBP should be required to comply with the requirements set out in Recommendation 13 (Criteria 13.1 – 13. 4)[46] in the following circumstances: a) Casinos (which includes internet casinos) and real estate agents – in the circumstances set out in R.13. b) Dealers in precious metals or stones - when they engage in any cash transaction equal to or above USD/€ 15,000[47]. c) 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 legal professional privilege or legal	

[46] 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.

[47] 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").

professional secrecy. 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 legal professional privilege or legal professional secrecy. It is for each jurisdiction to determine the matters that would fall under legal professional privilege or legal 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. d) 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; • 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 (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 criterion 16.1, the criteria set out under Recommendations 14, 15 and 21 should apply in relation to DNFBP.	
Additional elements 16.5 Is the reporting requirement extended to the rest of the professional activities of accountants, including auditing? 16.6 Are DNFBP required 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 domestically?	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

4.3 Regulation, supervision and monitoring (R. 24-25)

4.3.1 Description and Analysis

	Recommendation 24
General description of laws or other measures, the situation, or context.	
24.1 Countries should ensure that casinos (including Internet casinos) are subject to a comprehensive regulatory	

and supervisory regime that ensures they 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 AML/CFT regulatory and supervisory regime. The competent authority should have adequate powers to perform its functions, including powers to monitor and sanction (countries should ensure that criteria 17.1-17.4 apply to the obligations under R.12 and R.16).	
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) Adequate powers to perform its functions,	

[48] In assessing compliance with this criterion, assessors should have regard to Criteria 30.1 to 30.4 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).

including powers to monitor and sanction (countries should ensure that criteria 17.1-17.4 apply to the obligations under R.12 and R.16); b) have sufficient technical and other resources to perform its functions[48] .	
	Recommendation 25 (Guidance for DNFBPs other than guidance on STRs)
General description of laws or other measures, the situation, or context.	
25.1 Competent authorities should establish guidelines that will assist financial institutions and DNFBP to implement and comply with their respective AML/CFT requirements. For DNFBP, such guidelines may be established by SROs. At a minimum, the guidelines should give assistance on issues covered under the relevant FATF Recommendations, including: (i) a description of ML and FT techniques and methods; and (ii) any additional measures that these institutions and DNFBP could take to ensure that their AML/CFT measures are effective.	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

4.4 Other non-financial businesses and professions - Modern secure transaction techniques (R.20)

4.4.1 Description and Analysis

	Recommendation 20
General description of laws or other measures, the situation, or context.	
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 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 to money laundering include: • Reducing reliance on cash; • Not issuing very large denomination banknotes; • Secured automated transfer systems.	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

5. Legal Persons and Arrangements & Non-Profit Organisations

5.1 Legal Persons – Access to beneficial ownership and control information (R.33)

5.1.1 Description and Analysis

	Recommendation 33
General description of laws or other measures, the situation, or context.	
33.1 Countries should take measures to prevent the unlawful use of legal persons 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. Examples [49] of mechanisms that countries could use in seeking to ensure that there is adequate transparency may include: 1. A system of central registration (or up front disclosure system) 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. Relying on the investigative and other powers of law enforcement, regulatory, supervisory, or other competent authorities in a jurisdiction to obtain or have access to the information.	

[49] Note to assessors: These examples are summaries of mechanisms set out in the OECD Report "Behind the Corporate Veil. Using Corporate Entities for Illicit Purposes" 2001. An explanation of these mechanisms and their suitability is contained in the report itself.

These mechanisms are, to a large degree, complementary and countries may find it highly desirable and beneficial to use a combination of them. To the extent that countries rely on the investigative powers of their competent authorities, these authorities should have sufficiently strong compulsory powers for the purpose of obtaining the relevant information. Whatever mechanism is used it is essential that: (a) competent authorities are able to obtain or have access in a timely fashion to the beneficial ownership and control information, (b) the information is adequate, accurate and timely (see Criterion 33.2) and (c) competent authorities are able to share such information with other competent authorities domestically or internationally.	
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.	
33.3 Countries that have legal persons able to issue bearer shares 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 elements 33.4 Are measures in place 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?	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

34.1 Countries should take measures to prevent the unlawful use of legal arrangements 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. Examples [50] of mechanisms that countries could use in seeking to ensure that there is adequate transparency may include: 1. A system of central registration (or up front disclosure system) 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.	

[50] Note to assessors: These examples are summaries of mechanisms set out in the OECD Report "Behind the Corporate Veil. Using Corporate Entities for Illicit Purposes" 2001. An explanation of these mechanisms and their suitability is contained in the report itself.

3. Relying on the investigative and other powers of law enforcement, regulatory, supervisory, or other competent authorities in a jurisdiction to obtain or have access to the information. These mechanisms are, to a large degree, complementary and countries may find it highly desirable and beneficial to use a combination of them. To the extent that countries rely on the investigative powers of their competent authorities, these authorities should have sufficiently strong compulsory powers for the purpose of obtaining the relevant information. Whatever mechanism is used it is essential that: (a) competent authorities are able to obtain or have access in a timely fashion to the beneficial ownership and control information, (b) the information is adequate, accurate and timely (see Criterion 34.2) and (c) competent authorities are able to share such information with other competent authorities domestically or internationally.	
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, the trustee, and the beneficiaries of express trusts.	
Additional elements 34.3 Are measures in place 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?	
Additional material If you wish please indicate any other data or material	

you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and Analysis

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.	***Special Recommendation VIII***
General description of laws or other measures, the situation, or context.	
Reviews of the domestic non-profit sector: VIII.1 Countries should: (i) review the adequacy of domestic laws and regulations that relate to non-profit organisations; (ii) use all available sources of information to undertake domestic reviews of or have the capacity to obtain timely information on the activities, size and other relevant features of their non-profit sectors for the purpose of identifying the features and types of non-profit organisations (NPOs) that are at risk of being misused for terrorist financing by virtue of their activities or characteristics; and (iii) conduct periodic reassessments by reviewing new information on the sector's potential vulnerabilities to terrorist activities. Some examples of possible sources of information that could be used to undertake a domestic review or provide timely information on the activities, size and other relevant features of the domestic non-profit sector are: regulators, statistical institutions, tax authorities, FIUs, donor organisations, self-regulatory organizations	

or accreditation institutions, or law enforcement and intelligence authorities.	
Protecting the NPO sector from terrorist financing through outreach and effective oversight: VIII.2. Countries should undertake outreach to the NPO sector with a view to protecting the sector from terrorist financing abuse. This outreach should include i) raising awareness in the NPO sector about the risks of terrorist abuse and the available measures to protect against such abuse; and ii) promoting transparency, accountability, integrity, and public confidence in the administration and management of all NPOs.. An effective outreach program with the NPO sector may include the development of best practices to address terrorist financing risks, regular outreach events with the sector to discuss scope and methods of abuse of NPOs, emerging trends in terrorist financing and new protective measures, and the issuance of advisory papers and other useful resources.	
VIII.3 Countries should be able to demonstrate that the following steps have been taken to promote effective supervision or monitoring of those NPOs which account for: (i) a significant portion of the financial resources under control of the sector; and (ii) a substantial share of the sector's international activities	
VIII.3.1 NPOs should maintain information on: (1) the purpose and objectives of their stated activities; and (2) the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information should be publicly available either directly from the NPO or through appropriate	

authorities	
VIII.3.2 Countries should be able to demonstrate that there are appropriate measures in place to sanction violations of oversight measures or rules by NPOs or persons acting on behalf of NPOs. The application of such sanctions should not preclude parallel civil, administrative, or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate. Sanctions may include freezing of accounts, removal of trustees, fines, de-certification, de-licensing or de-registration.	
VIII.3.3 NPOs should be licensed or registered. This information should be available to competent authorities.[51]	
VIII.3.4 NPOs should maintain, for a period of at least five years, and make available to appropriate authorities, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation. This also applies to information mentioned in paragraphs (i) and (ii) of the Interpretative Note to Special Recommendation VIII	
Targeting and attacking terrorist abuse of NPOs through effective information gathering, investigation: VIII.4 Countries should implement measures to ensure that they can effectively investigate and gather information on NPOs.	
VIII.4.1 Countries should ensure effective domestic co-operation, co-ordination and information	

[51] Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favourable tax treatment (such as tax credits or tax exemptions).

sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs of potential terrorist financing concern.	
VIII.4.2 Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.	
VIII.4.3 Countries should develop and implement mechanisms for the prompt sharing of information among all relevant competent authorities in order to take preventative or investigative action when there is suspicion or reasonable grounds to suspect that a particular NPO is being exploited for terrorist financing purposes or is a front organization for terrorist fundraising. Countries should have investigative expertise and capability to examine those NPOs that are suspected of either being exploited by or actively supporting terrorist activity or terrorist organisations. Countries should also have mechanisms in place that allow for prompt investigative or preventative action against such NPOs.	
Responding to international requests for information about an NPO of concern: VIII.5 Countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs that are suspected of terrorist financing or other forms of terrorist support.	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of	

the AML/CFT system.	

6. National and International Co-operation

6.1 National co-operation and coordination (R.31 & 32)

6.1.1 Description and Analysis

	Recommendation 31
General description of laws or other measures, the situation, or context.	
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.	
<u>Additional elements</u> 31.2 Are mechanisms in place 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
32.1: Countries should review the effectiveness of their systems for combating money laundering and terrorist financing on a regular	

basis.	
R.30	***Resources (Policy makers)***
General description of laws or other measures, the situation, or context.	
30.1 Policy makers only: 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 influence or interference.	
30.2 Policy makers only: 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 Policy makers only: Staff of competent authorities should be provided with adequate and relevant training for combating ML and FT. Examples of issues to be covered under adequate and relevant training include: 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; the use of information technology and other resources relevant to the execution of their functions. Countries could also	

provide special training and/or certification for financial investigators for, inter alia, investigations of ML, FT, and the predicate offences.	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

	Recommendation 35 & Special Recommendation I
General description of laws or other measures, the situation, or context.	
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).[52].	
I.1 Countries should sign and ratify, or otherwise become a party to, and fully implement, the Terrorist Financing Convention[53].	
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) and its successor resolutions 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	

[52] Assessors should be satisfied that the following relevant articles of the Vienna Convention (Articles 3-11, 15, 17 and 19), the Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31, & 34), and the Terrorist Financing Convention (Articles 2-18) are fully implemented.

[53] 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.)

resolutions.	
Additional elements 35.2 Have 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 been signed, ratified or fully implemented?	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

6.3 Mutual Legal Assistance (R.36-38, SR.V, R.32)

Note to countries: In relation to SR.V, where the relevant information has already been fully described under R.36-38, it is only necessary to cross reference that material under the SR.V and to note any changes or differences of approach that may apply to terrorist financing.

6.3.1 Description and Analysis

	Recommendation 36
General description of laws or other measures, the situation, or context.	
36.1 Countries should be able to provide the widest possible range of mutual legal assistance in AML/CFT investigations, prosecutions and related proceedings. Mutual legal assistance should include assistance of the following nature: (a) the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons; (b) the taking of evidence or statements from persons; (c) providing originals or copies of relevant documents and records as well as any other information and	

evidentiary items, (d) effecting service of judicial documents; (e) facilitating the voluntary appearance of persons for the purpose of providing information or testimony to the requesting country and (f) 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[54]	
36.1.1 Countries should be able to provide such assistance in a timely, 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; overly strict interpretations of the principles of reciprocity and dual criminality.	
36.3 There should be clear and efficient processes for the execution of mutual legal assistance requests in a timely way and without undue delays.	
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	

[54] Elements (a) to (f) are drawn from the Palermo Convention.

impose secrecy or confidentiality requirements on financial institutions or DNFBP, except where the relevant information was obtained in circumstances where legal professional privilege or legal professional secrecy applies[55].	
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.	
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.	
Additional elements 36.8 Are the powers of competent authorities required under R.28 available for use when there is a direct request from foreign judicial or law enforcement authorities to domestic counterparts?	
	Recommendation 37 (dual criminality relating to mutual legal assistance)
General description of laws or other measures, the situation, or context.	
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	

[55] See also Criteria 16.2.

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
General description of laws or other measures, the situation, or context.	
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 Criterion 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 confiscation actions with other countries.	
38.4 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.	
38.5 Countries should consider authorising the sharing of confiscated assets between them when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.	

Additional elements 38.6 Are foreign non criminal confiscation orders (as described in criterion 3.7) recognised and enforced?	
V.1 Countries should ensure that Criteria 36.1 – 36.6 (in R.36) also apply to the obligations under SR.V.	***Special Recommendation V***
V.2 Countries should ensure that Criteria 37.1-37.2 (in R.37) also apply 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.	
R.30	***Resources (Central authority for sending/receiving mutual legal assistance/extradition requests)***
General description of laws or other measures, the situation, or context.	
30.1 Central authority for sending/receiving mutual legal assistance/extradition requests only: 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 influence or interference.	
30.2 Central authority for sending/receiving mutual legal assistance/extradition requests only: 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 Central authority for sending/receiving mutual legal assistance/extradition requests only: Staff of competent authorities should be provided with adequate and relevant training for combating ML and FT. Examples of issues to be covered under adequate and relevant training include: 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; the use of information technology and other resources relevant to the execution of their functions. Countries could also provide special training and/or certification for financial investigators for, inter alia, investigations of ML, FT, and the predicate offences.	
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: (c) Mutual legal assistance or other international requests for co-operation o 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 of the request,	***Recommendation 32***

whether it was granted or refused, and the time required to respond; If maintained, please provide these statistics	
Additional elements 32.3 Do competent authorities maintain comprehensive statistics on: c) other formal requests for assistance made or received by law enforcement authorities relating to ML or FT, including whether the request was granted or refused? If maintained, please provide these statistics	
V.6 Do additional elements 36.7 – 36.8 (in R.36) apply in relation to the obligations under SR.V? V.7 Do additional elements 38.4 – 38.6 (in R.38) apply in relation to the obligations under SR.V?	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

6.4 Extradition (R.39, 37 & SR.V)

6.4.1 Description and Analysis

	Recommendation 39
General description of laws or other measures, the situation, or context.	
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 the case referred to in criterion 39.2(b), 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 elements 39.5 Are simplified procedures of extradition in place by allowing direct transmission of extradition requests between appropriate ministries? Can persons be extradited based only on warrants of arrests or judgements? Is there a simplified procedure of extradition of consenting persons who waive formal extradition proceedings in place?	
	Recommendation 37 (dual criminality relating to extradition)
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.	
	Special Recommendation 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.	
Additional elements V.8 Does the additional element 39.5 (in R.39) apply extradition proceedings related to terrorist acts or FT?	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

6.5 Other Forms of International Co-operation (R.40, SR.V & R.32)

6.5.1 Description and Analysis

	Recommendation 40
General description of laws or other measures, the situation, or context.	
40.1 Countries should ensure that their competent authorities are	

able to provide the widest range of international cooperation to their foreign counterparts.	
40.1.1 Countries should be able to provide such assistance 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[56]. Examples of gateways, mechanisms or channels used in international cooperation and exchanges of information (other than MLA or extradition) include laws allowing exchanges of information on a reciprocal basis; bilateral or multilateral agreements or arrangements such as Memorandum of Understanding (MOU); 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	

[56] 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.

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 are authorised to conduct investigations on behalf of foreign counterparts; other competent authorities should be authorised to conduct investigations on behalf of foreign counterparts, where permitted by domestic law.	
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 legal professional privilege or legal professional secrecy applies[57]).	
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[58].	

[57] See also criteria 16.2

[58] 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.

Additional elements 40.10 Are mechanisms in place to permit a prompt and constructive exchange of information with non-counterparts? Does it take place directly or indirectly[59]? 40.10.1 Does the requesting authority as a matter of practice disclose to the requested authority the purpose of the request and on whose behalf the request is made? 40.11 Can the FIU obtain from other competent authorities or other persons relevant information requested by a foreign counterpart FIU?	
	Special Recommendation V:
V.5 Countries should ensure that Criteria 40.1 – 40.9 (in R.40) also apply to the obligations under SR.V.	
Additional elements V.9 Do additional elements 40.10 – 40.11 (in R.40) apply in relation to the obligations under SR.V?	
	Recommendation 32:
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: (c) Mutual legal assistance or other international requests for co-operation – …… o Other formal requests for assistance made or received by the FIU, including whether the request was granted or refused;	

[59] 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.

o Spontaneous referrals made by the FIU to foreign authorities. (d) Other action o Formal requests for assistance made or received by supervisors relating to or including AML/CFT, including whether the request was granted or refused. If maintained, please provide these statistics	
Additional elements 32.3 Do competent authorities maintain comprehensive statistics on: c) other formal requests for assistance made or received by law enforcement authorities relating to ML or FT, including whether the request was granted or refused?	
Additional material If you wish please indicate any other data or material you consider to be relevant to the effectiveness and efficiency of this part of the AML/CFT system.	

7. Other Issues

Countries may use this section to set out information on any additional measures or issues that are relevant to the AML/CFT system, and which are not covered elsewhere in this report.

Annex 2

MUTUAL EVALUATION/DETAILED ASSESSMENT REPORT
ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

[*NAME OF COUNTRY*]

REPORT TEMPLATE

[Date]

TABLE OF CONTENTS

PREFACE - information and methodology used for the evaluation of [Country]

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of [*Country*[60]] was based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004[61]. The evaluation was based on the laws, regulations and other materials supplied by [*Country*], and information obtained by the evaluation team during its on-site visit to [*Country*] from [*dates*], and subsequently. During the on-site the evaluation team met with officials and representatives of all relevant [C*ountry*] government agencies and the private sector. A list of the bodies met is set out in Annex XX to the mutual evaluation report.

2. The evaluation was conducted by an assessment team, which consisted of members of the FATF Secretariat and FATF experts in criminal law, law enforcement and regulatory issues: [*list names* from the FATF Secretariat][*list names and agencies of examiners and their role e.g. legal expert*]. The experts reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all these systems.

3. This report provides a summary of the AML/CFT measures in place in [*Country*] as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, sets out [*Country*] levels of compliance with the FATF 40+9 Recommendations (see Table 1), and provides recommendations on how certain aspects of the system could be strengthened (see Table 2).

[60] All references to country apply equally to territories or jurisdictions.

[61] As updated in …..

Executive Summary

The Executive Summary is the only summary of the mutual evaluation report that is prepared, and will provide the text for any summary that is published. For the purposes of the preparation of the Report on Standards and Codes (ROSC), the substantive text of the Executive Summary will remain unchanged, but certain formal paragraphs could be added or changes made.

The text of the Executive Summary should summarise the main findings under each of the sections of the mutual evaluation/detailed assessment report and using the order of the sections contained in the report. Normally an executive summary should not be more than 15 pages, and should contain the sub-headings set out below.

The Executive Summary should also begin with the following proforma paragraph, and then very briefly (2-3 paragraphs) describe the report's overall findings on the AML/CFT system in the country and the effectiveness of that system.

> "This report provides a summary of the AML/CFT measures in place in [name of assessed country] as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, and provides recommendations on how certain aspects of the system could be strengthened. It also sets out [name of assessed country] levels of compliance with the FATF 40+9 Recommendations (see the attached table on the Ratings of Compliance with the FATF Recommendations)."

1. **Background Information**
2. **Legal Systems and Related Institutional Measures**
3. **Preventive Measures – Financial Institutions**
4. **Preventive Measures – Designated Non-Financial Businesses and Professions**
5. **Legal Persons and Arrangements & Non-Profit Organisations**
6. **National and International Co-operation**
7. **Other Issues**

Table 1: Ratings of Compliance with FATF Recommendations
Table 3: Authorities' Response to the Evaluation (if necessary)

MUTUAL EVALUATION REPORT

1. GENERAL

1.1 General information on [*country*]

This section should contain general information on the country. Examples of the type of information to include are whether there is a federal or unitary system of government, the type of government, the type of legal system, whether there is a Constitution, and whether the country is subject to supranational laws or regulations (as in the European Union). Where significant weaknesses or shortcomings are detected, it should also set out a short summary addressing the structural elements referred to in paragraph 7 of the AML/CFT Methodology 2004:

a) the respect of principles such as transparency and good governance;
b) a proper culture of AML/CFT compliance shared and reinforced by government, financial institutions, designated non-financial businesses and professions; industry trade groups, and self-regulatory organisations (SROs);
c) appropriate measures to combat corruption;
d) a reasonably efficient court system that ensures that judicial decisions are properly enforced;
e) high ethical and professional requirements for police officers, prosecutors, judges, etc. and measures and mechanisms to ensure these are observed;
f) 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.

1.2 General Situation of Money Laundering and Financing of Terrorism

This section provides background information on vulnerabilities within [*country*] to money laundering and the financing of terrorism, trends regarding criminal activity in general, including financing of terrorism, the types of predicate offences that are generating illegal proceeds that are laundered (whether those offences are domestic or foreign), any estimates of the amount of money being laundered, and the methods, techniques and trends that have been observed regarding the laundering. Information should also be provided on any terrorist activity that has occurred within the country, and on the sources and methods used to finance terrorist activity. Assessors should highlight specific matters of concern, and in particular should set out the vulnerabilities having regard to the institutional structures, the geographic location, the financial markets etc. Assessors should also, when necessary, list any potential future AML/CFT vulnerabilities.

1.3 Overview of the Financial Sector and DNFBP

This section should contain a description of the types of financial institutions operating in the country, and listing the financial activities (see the definition of "financial institution" in the Methodology) that they engage in or are authorised to engage in. There should also be similar information on DNFBP and the activities that they generally engage in. Finally, the section should set out information on the number and size of financial institutions and DNFBP, and any recent changes of significance e.g. consolidation in a particular sector.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements

This section should contain a description of the types of legal persons and legal arrangements (referred to here as "entities") that can be established or created, or can own property, in the country. It should provide information on the basic characteristics of such entities e.g. who has ownership (for example shareholders, which could be legal or natural persons) and control (e.g. directors) and whether and where they are registered and/or require a registered office or agent. Please provide information on the extent to which such entities are prevalent, statistics on numbers and information on their significance, if available, within the financial sector.

1.5 Overview of strategy to prevent money laundering and terrorist financing

a. AML/CFT Strategies and Priorities

- This section should set out the current main policies and objectives of the government for combating money laundering or terrorist financing. It should describe the priorities, and state whether the objectives are being achieved.

b. The institutional framework for combating money laundering and terrorist financing

This section should provide a brief overview of the government and non-government Ministries, regulatory and other authorities and other bodies involved in combating money laundering or terrorist financing.

c. Approach concerning risk

This section should provide an overview of the policy and procedures that the authorities may have adopted in applying a risk-based approach to combating money laundering and terrorist financing. It should describe the authorities' overall philosophy towards a risk-based approach (e.g. does it form an integral part of its regulatory framework?), and it should indicate how the relevant risk assessments are undertaken to help determine the policy and its practical application. Finally, there should be a description of the mechanism by which any permitted variations from the generally applicable standards are promulgated, and what arrangements, if any, are in place to monitor the continuing suitability of the exceptions.

d. Progress since the last mutual evaluation

Where a country has undergone a previous mutual evaluation or detailed assessment, this section should summarise the key findings and/or recommendations that were made in the previous report, and set out the measures that the country had taken to address the recommendations in the period up to the date of the on-site visit or immediately thereafter.

2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalisation of Money Laundering (R.1 & 2)

2.1.1 Description and Analysis62
2.1.2 Recommendations and Comments
2.1.3 Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating[63]
R.1		
R.2		

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis
2.2.2 Recommendations and Comments
2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II		

2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)

2.3.1 Description and Analysis
2.3.2 Recommendations and Comments
2.3.3 Compliance with Recommendations 3

	Rating	Summary of factors underlying rating
R.3		

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and Analysis
2.4.2 Recommendations and Comments
2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III		

Authorities

[62] Note to assessors: for all Recommendations, the description and analysis section should include the analysis of effectiveness, and should contain any relevant statistical data.

[63] These factors are only required to be set out when the rating is less than Compliant.

2.5 The Financial Intelligence Unit and its functions (R.26)

2.5.1 Description and Analysis
2.5.2 Recommendations and Comments
2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26		

2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27 & 28)

2.6.1 Description and Analysis
2.6.2 Recommendations and Comments
2.6.3 Compliance with Recommendations 27 & 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27		
R.28		

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis
2.7.2 Recommendations and Comments
2.7.3 Compliance with Special Recommendation IX

	Rating	Summary of factors relevant to s.2.7 underlying overall rating
SR.IX		

3. PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

Customer Due Diligence & Record Keeping

3.1 Risk of money laundering or terrorist financing

A country may decide not to apply certain AML/CFT requirements, or to reduce or simplify the measures being taken, on the basis that there is low or little risk of money laundering or terrorist financing. Similarly, as set out in R.5, financial institutions may, in certain circumstances determine the degree of risk attached to particular types of customers, business relationships, transactions or products. Section 3.1 should set out the basis upon which the country has taken its decision where it has decided not to apply the required AML/CFT measures to a particular financial sector. Where there are specific references to risk in individual Recommendations (see Instructions to Assessors) the issue of risk for those Recommendations should be covered in the relevant section of the MER i.e. sections 3.2, 3.8, 3.13 and 4.1, 4.4 and 4.5. Assessors should analyse these decisions, review the process by which risk is assessed, and assess the reasonableness of the conclusions. They may also make recommendations or comments. See AML/CFT Methodology 2004, paragraphs 17-18.

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)

3.2.1 Description and Analysis
3.2.2 Recommendations and Comments
3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5		
R.6		
R.7		
R.8		

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis
3.3.2 Recommendations and Comments
3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9		

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis
3.4.2 Recommendations and Comments
3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4		

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis
3.5.2 Recommendations and Comments
3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10		
SR.VII		

Unusual and Suspicious Transactions

3.6 Monitoring of transactions and relationships (R.11 & 21)

3.6.1 Description and Analysis
3.6.2 Recommendations and Comments
3.6.3 Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating
R.11		
R.21		

3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)

3.7.1 Description and Analysis[64]
3.7.2 Recommendations and Comments
3.7.3 Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13		
R.14		
R.19		
R.25		
SR.IV		

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)

3.8.1 Description and Analysis
3.8.2 Recommendations and Comments
3.8.3 Compliance with Recommendations 15 & 22

[64] The description of the system for reporting suspicious transactions in s.3.7 is integrally linked with the description of the FIU in s.2.5, and the two texts need to be complementary and not duplicative.

	Rating	Summary of factors underlying rating
R.15		
R.22		

3.9 Shell banks (R.18)

3.9.1 Description and Analysis
3.9.2 Recommendations and Comments
3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18		

Regulation, supervision, guidance, monitoring and sanctions

3.10 The supervisory and oversight system - competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)

3.10.1 Description and Analysis
3.10.2 Recommendations and Comments
3.10.3 Compliance with Recommendations 23, 29, 17 & 25

Note to assessors - in completing this section of the report, assessors should address the various elements of the regulatory system and the relevant Recommendations, in the following sequence:

1. Describe and analyse all the competent authorities and SROs, and their roles, functions and duties in regulating the application of AML/CFT measures in the financial system, as well as describing their organisational structures and resources (R.23, R.30 - in particular criteria 23.1, 23.2, 30.1-30.3).
2. Set out and analyse the relevant powers (including sanction powers) of each authority and any other sanctions that are applicable for breaches of AML/CFT requirements (R.29, R.17 - all criteria).
3. Describe and analyse how market entry is regulated and how the authorities check the ownership/control of financial institutions regarding criminal records and where appropriate, fitness and properness (R.23 - in particular criteria 23.3, 23.3.1, 23.5 & 23.7 (licensing/registration elements only)).
4. Describe and analyse the process of ongoing supervision and monitoring, and include any available statistics regarding on-site or off-site inspections (R.23, R.32 - in particular criteria 23.4, 23.6, 23.7 (supervision/oversight elements only), 32.2d)
5. Explain and analyse any AML/CFT guidance/guidelines that have been provided by competent authorities to financial institutions (R.25 - criteria 25.1 only).
6. Provide ratings and factors underlying the ratings for Recommendations 17, 23, 25 and 29

	Rating	Summary of factors relevant to s.3.10 underlying overall rating
R.17		
R.23		
R.25		

R.29		

3.11 Money or value transfer services (SR.VI)

This section should very briefly summarise and cross-reference the description and analysis that has been made elsewhere in section 4 on money or value transfer services. It should then set out in full any recommendations or comments, and the material concerning the compliance rating.

3.11.1 Description and Analysis (summary)
3.11.2 Recommendations and Comments
3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI		

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

4.1 Customer due diligence and record-keeping (R.12)
(applying R.5, 6, and 8 to 11)

Note to assessors - in completing this section of the report, assessors should seek to address the various elements of customer due diligence, record-keeping and monitoring and the relevant Recommendations, in the following sequence:

1. Describe and analyse the customer due diligence requirements and measures for DNFBP (applying R.5, 6, 8 & 9). Where requirements have already been described in Section 3 of the MER, it is only necessary to cross reference that material and to note any changes or differences of approach that may apply to DNFBP.
2. Set out and analyse the record-keeping requirements for DNFBP (applying R.10). Again this may be done in whole or part by cross-referencing.
3. Indicate if there are any differences for DNFBP regarding monitoring (applying R.11) analyse those.

4.1.1 Description and Analysis
4.1.2 Recommendations and Comments
4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12		

4.2 Suspicious transaction reporting (R.16)

(applying R.13 to 15 & 21)

Note to assessors - in completing this section of the report, assessors should seek to address the various elements of monitoring and reporting system and the relevant Recommendations, in the following sequence:

1. Describe and analyse the suspicious transaction reporting system for DNFBP (applying R.13-14). Where the reporting obligations have already been fully described in Section 3 of the MER, it is only necessary to cross reference that material and to note any changes or differences of approach that may apply to DNFBP.
2. Set out and analyse the internal control requirements for DNFBP (applying R.15). Again this may be done in whole or part by cross-referencing.
3. Indicate if there are any differences for DNFBP regarding the application of R.21, and analyse these.

4.2.1 Description and Analysis
4.2.2 Recommendations and Comments
4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16		

4.3 Regulation, supervision and monitoring (R.24-25)

4.3.1 Description and Analysis
4.3.2 Recommendations and Comments
4.3.3 Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24		
R.25		

4.4 Other non-financial businesses and professions Modern secure transaction techniques (R.20)

4.4.1 Description and Analysis
4.4.2 Recommendations and Comments
4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20		

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS

5.1 Legal Persons – Access to beneficial ownership and control information (R.33)

5.1.1 Description and Analysis
5.1.2 Recommendations and Comments
5.1.3 Compliance with Recommendations 33

	Rating	Summary of factors underlying rating
R.33		

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis
5.2.2 Recommendations and Comments
5.2.3 Compliance with Recommendations 34

	Rating	Summary of factors underlying rating
R.34		

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and Analysis
5.3.2 Recommendations and Comments
5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII		

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and coordination (R.31 & R.32)

6.1.1 Description and Analysis
6.1.2 Recommendations and Comments
6.1.3 Compliance with Recommendation 31 & 32 (criterion 32.1 only)

	Rating	Summary of factors underlying rating
R.31		
R.32		

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis
6.2.2 Recommendations and Comments
6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35		
SR.I		

6.3 Mutual Legal Assistance (R.36-38, SR.V)

6.3.1 Description and Analysis

6.3.2 Recommendations and Comments
6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
R.36		
R.37		
R.38		
SR.V		

6.4 Extradition (R.37, 39, SR.V)

6.4.1 Description and Analysis
6.4.2 Recommendations and Comments
6.4.3 Compliance with Recommendations 37 & 39, and Special Recommendation V

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
R.39		
R.37		
SR.V		

6.5 Other Forms of International Co-operation (R.40 & SR.V)

6.5.1 Description and Analysis
6.5.2 Recommendations and Comments
6.5.3 Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.5 underlying overall rating
R.40		
SR.V		

7. OTHER ISSUES

7.1 Resources and statistics

Assessors should use this section as follows. The text of the description, analysis and recommendations for improvement that relate to Recommendations 30 and 32 is contained in all the relevant sections of the report i.e. all of section 2, parts of sections 3 and 4, and in section 6. There is a single rating for each of these Recommendations, even though the Recommendations are addressed in several sections. Section 7.1 of the report will contain only the box showing the rating and the factors underlying the rating, and the factors should clearly state the nature of the deficiency, and should cross refer to the relevant section and paragraph in the report where this is described.

	Rating	Summary of factors relevant to Recommendations 30 and 32 and

		underlying overall rating
R.30		
R.32		

7.2 Other relevant AML/CFT measures or issues

Assessors may use this section to set out information on any additional measures or issues that are relevant to the AML/CFT system in the country being evaluated, and which are not covered elsewhere in this report.

7.3 General framework for AML/CFT system (see also section 1.1)

Assessors may use this section to comment on any aspect of the general legal and institutional framework within which the AML/CFT measures are set, and particularly with respect to any structural elements set out in section 1.1, where they believe that these elements of the general framework significantly impair or inhibit the effectiveness of the AML/CFT system.

TABLES

Table 1: Ratings of Compliance with FATF Recommendations
Table 2: Recommended Action Plan to improve the AML/CFT system
Table 3: Authorities' Response to the Evaluation (if necessary)

Table 1. Ratings of Compliance with FATF Recommendations

The rating of compliance vis-à-vis the FATF Recommendations should be made according to the four levels of compliance mentioned in the 2004 Methodology (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC)), or could, in exceptional cases, be marked as not applicable (na).

Forty Recommendations	Rating	Summary of factors underlying rating[65]
Legal systems		
1. ML offence		
2. ML offence – mental element and corporate liability		
3. Confiscation and provisional measures		
Preventive measures		
4. Secrecy laws consistent with the Recommendations		
5. Customer due diligence		
6. Politically exposed persons		
7. Correspondent banking		
8. New technologies & non face-to-face business		
9. Third parties and introducers		
10. Record keeping		
11. Unusual transactions		
12. DNFBP – R.5, 6, 8-11		
13. Suspicious transaction reporting		
14. Protection & no tipping-off		
15. Internal controls, compliance & audit		
16. DNFBP – R.13-15 & 21		
17. Sanctions		
18. Shell banks		
19. Other forms of reporting		
20. Other NFBP & secure transaction techniques		
21. Special attention for higher risk countries		
22. Foreign branches & subsidiaries		
23. Regulation, supervision and		

[65] These factors are only required to be set out when the rating is less than Compliant.

monitoring		
24. DNFBP - regulation, supervision and monitoring		
25. Guidelines & Feedback		
Institutional and other measures		
26. The FIU		
27. Law enforcement authorities		
28. Powers of competent authorities		
29. Supervisors		
30. Resources, integrity and training		
31. National co-operation		
32. Statistics		
33. Legal persons – beneficial owners		
34. Legal arrangements – beneficial owners		
International Co-operation		
35. Conventions		
36. Mutual legal assistance (MLA)		
37. Dual criminality		
38. MLA on confiscation and freezing		
39. Extradition		
40. Other forms of co-operation		
Nine Special Recommendations	**Rating**	**Summary of factors underlying rating**
SR.I Implement UN instruments		
SR.II Criminalise terrorist financing		
SR.III Freeze and confiscate terrorist assets		
SR.IV Suspicious transaction reporting		
SR.V International co-operation		
SR VI AML requirements for money/value transfer services		
SR VII Wire transfer rules		
SR.VIII Non-profit organisations		
SR.IX Cross Border Declaration & Disclosure		

Table 2: Recommended Action Plan to Improve the AML/CFT System

AML/CFT System	Recommended Action (listed in order of priority)
1. General	**No text required**
2. Legal System and Related Institutional Measures	
2.1 Criminalisation of Money Laundering (R.1 & 2)	
2.2 Criminalisation of Terrorist Financing (SR.I)	
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	
2.4 Freezing of funds used for terrorist financing (SR.III)	
2.5 The Financial Intelligence Unit and its functions (R.26)	
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	
2.7 Cross Border Declaration & Disclosure	
3. Preventive Measures – Financial Institutions	
3.1 Risk of money laundering or terrorist financing	
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)	
3.3 Third parties and introduced business (R.9)	
3.4 Financial institution secrecy or confidentiality (R.4)	
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	
3.6 Monitoring of transactions and relationships (R.11 & 21)	
3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	
3.8 Internal controls, compliance, audit and foreign branches (R.15 &	

22)	
3.9 Shell banks (R.18)	
3.10 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	
3.11 Money value transfer services (SR.VI)	
4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	
4.2 Suspicious transaction reporting (R.16)	
4.3 Regulation, supervision and monitoring (R.24-25)	
4.4 Other non-financial businesses and professions (R.20)	
5. Legal Persons and Arrangements & Non-Profit Organisations	
5.1 Legal Persons – Access to beneficial ownership and control information (R.33)	
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)	
5.3 Non-profit organisations (SR.VIII)	
6. National and International Co-operation	
6.1 National co-operation and coordination (R.31)	
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	
6.3 Mutual Legal Assistance (R.36-38 & SR.V)	
6.4 Extradition (R.39, 37 & SR.V)	
6.5 Other Forms of Co-operation (R.40 & SR.V)	
7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	
7.2 Other relevant AML/CFT	

measures or issues	
7.3 General framework – structural issues	

Table 3: Authorities' Response to the Evaluation (if necessary)

Relevant sections and paragraphs	Country Comments

ANNEXES

Annex 1: **List of abbreviations**
Annex 2: **Details of all bodies met on the on-site mission - Ministries, other government authorities or bodies, private sector representatives and others.**
Annex 3: **Copies of key laws, regulations and other measures**
Annex 4: **List of all laws, regulations and other material received**

Annex 3

Factors or elements that could be relevant to whether individual recommendations are effectively implemented

For the recommendations listed below, assessors, based on the specific ML/TF risks and situation in the country, could take into account the following factors or elements in their analysis of effectiveness, including for the rating:

MER – SECTION 2

***Laws and Regulations** (R.1, 2, 3, SR II & III)*

1. Data and other information on prosecutions, convictions, penalties, freezing/seizing and confiscation etc (especially those required under R.32);
2. Current criminal law policy and legal practice in relation to R.1, 2 and SR II, i.e.:
   - the drafting of ML/TF offences and any judicial interpretation;
   - the evidentiary standards currently applied;
   - level of resources dedicated to the ML/TF related investigations and prosecutions;
3. The nature of the law enforcement/prosecutorial or other organisational structures for the investigation, seizing/freezing, and confiscation of the proceeds of crime and freezing of funds used for terrorist financing (R.3 and SR III):
   - whether specific mechanisms focussed on proceeds of crime exist and the legal and practical capacity to act expeditiously to freeze/seize criminal proceeds;
   - examples of in practice delay in the freezing/unfreezing of the assets of listed persons;
   - sanctions applied for failure to properly implement obligations in relation to SR.III;

***Authorities** (R.26 & 27 and SR.IX)*

1. Results: (a) in relation to the FIU (processing of STR, number received vs. number referred to competent authorities, etc.), (b) in relation to law enforcement authorities (ML/TF investigations initiated, etc.), (c) in relation to SR IX (number of reports made and value of the amounts seized/confiscated and number of operations aimed at identifying/targeting illicit cash couriers);
2. Structural issues: (a) FIU structure and location; (b) law enforcement/prosecutorial authorities institutional framework; (c) adequate institutional framework to support the declaration/disclosure system and (d) for all competent authorities: resources, capacity/expertise and quality of inter-agency co-ordination;
3. FIU access to information (including law enforcement and commercial databases) and FIU relationship with financial sector and DNFBPs including feedback.

MER – SECTIONS 3 & 4

***Customer Due Diligence, Record Keeping, and Internal Controls** (R.4-11, 15, 18, 21-22, SR VI & VII for financial institutions, R.12 for DNFBPs)*

1. Number, nature and outcomes of interventions at financial institutions and DNFBPs, and outcomes of meetings with financial institutions and DNFBPs;
2. Compliance failures identified by the regulatory examination programme[66].

[66] Please note that a lack of supervisory action is not per se indicative of whether the Recommendations have been effectively implemented or not.

Suspicious Transactions (R.13 & SR IV for financial institutions, R.16 for DNFBPs)
1. Quantity of STR - Data and other information on STRs, including appropriate breakdowns.
2. Quality of STR (number of STRs used in investigations, result of supervision programme, etc.).

Supervision and oversight (R.17, 23, 25 & 29 and SR VI for financial institutions and R.24 for DNFBPs)

1. Results.
   - in relation to R.17 and SR.VI - the number of cases where sanctions have been applied (taking into account the number of supervisory compliance checks), the nature of the failings and the type of sanctions applied (to check the appropriateness/proportionality of the sanctions imposed)[67];
   - in relation to R.23 & 29 - the number of on-site supervisory inspections that covered AML/CFT issues; the frequency and duration of inspections; the types and range of institutions inspected having regard to ML/TF risks; the nature of the on-site inspection, the use of other supervisory techniques; and the results in terms of compliance by financial institutions;

2. Supervisor's powers of enforcement and sanction in relation to R.23 & 29: (a) the dissuasive nature and scope of sanctions; (b) for inspections, the existence of written guidelines or regulations describing the procedure to follow; (c) possibility or not of giving prior notice of inspections; (d) existence of sanctions for refusing to disclose information to the supervisor, etc.
3. Structural issues in relation to R.23 and SR VI: adequate institutional framework; general organisation of supervisory bodies; adequate resources (financial, staff, technical, etc. especially for the authorities responsible for registering /licensing under SR VI) and adequate capacity/expertise (including staff background, training and professional standards) (see also R.30).
4. Guidance **(**R.25) – whether there is guidance for the different types of financial institutions, both general and in relation to STRs specifically, as well as the provision of adequate specific/general feedback on STRs. Effective guidance is also normally partially generic to all institutions and partially specific to particular types of institutions, businesses and professions.
5. Awareness Raising (Rec. 25, SR VI and SR VIII): number of awareness raising campaigns and seminars conducted.

MER – SECTION 6
International Cooperation (R.36, 38, 39 & R.40)

The following elements could equally apply to mutual legal assistance (R.36), assistance in freezing, seizing and confiscation (R.38) and extradition (R.39).

1. Legal requirements: (a) dual criminality as a pre-condition: whether it may inhibit the capacity to provide assistance e.g. whether the laundering of the proceeds of full range of predicate offences is a crime, and if not, whether assistance can be provided to other countries; (b) whether the type of assistance under R.36, 38 & 39 can be provided without a treaty or agreement, and if so, under what conditions; (c) the number and types of grounds for refusing assistance;
2. Results: (a) the existence of multilateral or bilateral treaties or agreements, whether co-operation can take place in the absence of such treaties, and will these allow the country to provide assistance to the other countries that are likely to seek its assistance; (b) the number/type of cases where assistance has been refused; (c) existing figures in relation to C.32.2(c); (d) the resources available to process and act upon assistance requests and (e) the simplicity/ease of the process.

In relation to R.40: (a) the quantitative information required to be collected under Recommendation 32; (b) reasons for refusing the exchange of information; (c) proportionality of safeguard systems used to limit the use of exchanged information to protect privacy; (d) nature of prohibitions on the use of data;

[67] Assessors should note that only having criminal sanctions for non-compliance with preventive requirements is unlikely to be sufficient by itself. Normally, a country would have an adequate range of administrative sanctions for financial institution non-compliance exercised by a competent authority.

(e) number/conditions of use of MOUs; (f) time required to respond to requests, and quality of information provided.