IMMEDIATE ATTENTION

SM/02/349

November 8, 2002

To: Members of the Executive Board

From: The Secretary

Subject: **Report on the Outcome of the FATF Plenary Meeting and Proposal for the Endorsement of the Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Standard**

Attached for consideration by the Executive Directors is a report on the outcome of the FATF Plenary meeting and proposal for the endorsement of the methodology for assessing compliance with anti-money laundering and combating the financing of terrorism (AML/CFT) standard. It is intended that this paper will be published on the Fund's external website after **November 15, 2002.**

It is not proposed to bring this matter to the agenda of the Executive Board for discussion unless an Executive Director so requests by **noon on Friday, November 15, 2002**. In the absence of such a request, the draft decisions that appear on page 4 will be deemed approved by the Executive Board and it will be so recorded in the minutes of the next meeting thereafter.

Questions may be referred to Mr. M. Moore, MAE (ext. 38631) and Mr. Kyriakos-Saad, LEG (ext. 34286).

Att: (1)

Other Distribution:
Department Heads

INTERNATIONAL MONETARY FUND

Report on the Outcome of the FATF Plenary Meeting and Proposal for the Endorsement of the Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Standard

Prepared by the Monetary and Exchange Affairs and Legal Departments

Approved by François Gianviti and Stefan Ingves

November 8, 2002

I. Introduction

1. This paper reports on the outcome of the discussions with the Financial Action Task Force (FATF) at its plenary meetings from October 9–11, 2002, and seeks endorsement by the Executive Board of the final anti-money laundering and combating the financing of terrorism (AML/CFT) Methodology. At the plenary, the FATF endorsed the AML/CFT methodology and agreed to the four conditions set out by the Executive Board, July 26, 2002. At the July Board meeting, Directors requested that the methodology be presented for the Executive Board's endorsement following the endorsement at the FATF plenary.[1]

2. In the sections that follow, Section II provides background on the results of the July 26, 2002, Board discussion and Section III describes the outcome of the FATF plenary meeting, including the adoption of the anti-money laundering methodology and the 12-month pilot program of assessments and the preparation of associated Reports on the Observance of Standards and Codes (ROSCs). Section IV proposes two decisions for Executive Directors.

II. Background

3. On July 26, 2002, the Executive Board discussed the paper *"Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), Proposals to assess a Global Standard and to Prepare ROSCs"* (SM/02/227, July 17, 2002). Directors agreed to:

- **Conditionally** add the Financial Action Task Force (FATF) 40 Recommendations against money laundering and the 8 Special Recommendations on terrorism financing (FATF 40+ 8) to the list of areas and associated standards and codes useful to the operational work of the Fund; and

[1] The staff of the World Bank is sending to its Board a report for information on the outcome of the FATF Plenary Meetings. The Bank's Board did not request other action.

- Endorse a 12-month pilot program of AML/CFT assessments and accompanying **ROSCs** that would involve participation of the Fund and the World Bank, the Financial Action Task Force, and FATF-Style Regional Bodies (FSRBs).

4. In the summing up of the Board discussion (BUFF/02/122, July 31, 2002), Directors emphasized that four key **principles** should guide the Fund's role in AML/CFT assessments and accompanying ROSCs:

- the staff's involvement in assessing non-prudentially-regulated financial sector activities should be confined to those that are macro-economically relevant and pose a significant risk of money laundering/terrorism financing;

- all assessment procedures should be transparent and consistent with the mandate and core expertise of the different institutions involved, and compatible with the uniform, voluntary, and cooperative nature of the ROSC exercise;

- the assessments should be followed up with appropriate technical assistance at the request of the countries assessed in order to build their institutional capacity and develop their financial sectors; and

- the assessments would be conducted in accordance with the comprehensive and integrated methodology.

5. Directors endorsed adding AML/CFT to the list of 11 areas where standards and codes are useful to the operational work of the Fund and for which assessments are undertaken, and to adopt the FATF 40+8 Recommendations as the associated standard, provided that four **conditions** are met:

- the FATF Secretariat, in consultation with Fund and Bank staff, satisfactorily completes the draft of the comprehensive and integrated assessment methodology by the Annual Meetings for consideration at the October FATF Plenary;

- the FATF endorses in its October Plenary the comprehensive and integrated assessment methodology and its use in undertaking FATF/FSRB mutual evaluations and Fund/Bank staff-led assessments;

- the FATF agrees in its October Plenary to undertake its mutual evaluations consistent with the ROSC process as elaborated in Section II of SM/02/227; and

- the FATF does not undertake a further round of the non-cooperative countries and territories (NCCT) initiative, at least during the period of the 12-month pilot project.

III. Outcome from the FATF Plenary Meeting

6. At the October plenary, the FATF endorsed the comprehensive and integrated methodology and agreed to the other conditions as outlined above. During the plenary discussion the FATF President, Mr. Jochen Sanio stated that the FATF Plenary had formally agreed to the four conditions. Mr. Sanio subsequently confirmed the decision of the FATF Plenary in an October 24, 2002 letter to Fund Management (attached Annex I). The letter notes the endorsement of the AML/CFT methodology and participation by the FATF in the 12-month pilot program together with the IMF and the World Bank. The letter states that the new methodology would be used for future mutual evaluations, and confirms that then FATF would not undertake a further round of the NCCT process during the 12-month pilot program. In staff's view the four conditions set by the Board have been met.

7. Since the circulation to the Board of the August 26, 2002 version of the AML/CFT methodology, there have been two further drafts circulated to FATF members and observer organizations for comments. The draft AML/CFT methodology was again discussed and commented upon during two readings at the October plenary, resulting in the final version endorsed by the plenary. Attached to this paper for reference is a redline version of the final draft of the AML/CFT methodology, which shows the changes since the August version circulated to the Board (attached as Annex II). Among the changes, the FATF has added a new criterion 41 that takes verbatim the language of FATF Special Recommendation V. In staff's view, all of the changes adopted in the final methodology are acceptable, as they are largely technical and do not expand the scope of AML/CFT assessments beyond the areas of money laundering or the financing of terrorism as discussed and agreed by the Fund Board.

8. There is not yet a decision by the FATF on which FATF members would be subject to FATF mutual evaluations. Staff is following up with the FATF to ensure that there is an adequate sample of FATF-led assessments using the comprehensive AML/CFT methodology. In addition, staff continues to work with the FSRBs to encourage their participation in the pilot program. Some FSRBs have indicated that participation in the program is likely, whereas others are expressing some concerns about the effect of the on-going process on their work program for mutual evaluations.

9. During the Plenary the FATF reviewed progress by jurisdictions identified in the first two rounds of the NCCT exercise and removed four countries from the NCCT list. The FATF concluded that progress by two countries on the existing list had been inadequate and proposed further counter-measures if remedial legislation is not enacted by December 15, 2002[2]. The fourth condition set by the Board for adding AML/CFT to the list of 11 areas where standards and codes are useful for the operational work of the Fund and to undertake assessments was that the FATF would not undertake "a further round of the non-cooperative countries and territories (NCCT) initiative, at least during the period of the 12-month pilot project." Prior to setting that condition in the Executive Board Seminar on June 27, 2002, the

---

[2] Countermeasures could include the possibility of enhanced surveillance and reporting of financial transactions and other relevant actions.

staff (Buff/02/89) clarified that a "further round of the NCCT process" is "a review of *a new set of countries"* and that the FATF, in agreeing not to undertake a third round, "was not renouncing the NCCT process, and that the current process of listing, monitoring or reviewing any of the forty-six countries assessed under the first two rounds would continue." This point was emphasized by Mr. Sanio, the then FATF President-elect, in his statement at the Board seminar. The FATF's October 24, 2002, letter restates this position. Therefore, the decision by FATF to propose counter-measures against two countries does not represent "a further round of the NCCT initiative" as the decision is based on the FATF's ongoing monitoring of jurisdictions that it had previously listed as NCCTs during the first two rounds, and does not breach the forth condition set by the Board.

IV. Proposed Decisions for Directors

The following draft decisions are proposed for adoption by the Executive Board:

10. Executive Directors take note that the conditions set forth in BUFF/02/122 are met and add the FATF 40+8 Recommendations to the list of areas and associated standards and codes useful to the operational work of the Fund for which assessments will be undertaken and reports on the Observance of Standards and Codes (ROSCs) will be prepared.

11. Executive Directors endorse the comprehensive and integrated methodology that was endorsed at the FATF October 2002 Plenary.

ANNEX I

FATF•GAFI

Financial Action Task Force on Money Laundering
Groupe d'Action Financière sur le Blanchiment de Capitaux

FATF Secretariat,
Secrétariat du GAFI,
2, rue André-Pascal
75775 Paris Cedex 16, France

Telephone: (+33-1) 45 24 79 45
Fax: (+33-1) 45 24 17 60
E-mail: contact@fatf-gafi.org

THE PRESIDENT

Mr. Horst Köhler
Managing Director
International Monetary Fund
700 19th Street, NW
Washington D.C. 20431
United States

Fax: 1 202 623 6214

24 October 2002

Dear Mr. Köhler,

Thank you for your letter of 7 August 2002 concerning the preparation of comprehensive anti-money laundering (AML) countering the financing of terrorism (CFT) assessments, and the IMF's commitment to conduct a pilot AML/CFT assessment programme. On behalf of the FATF, I welcome the IMF's recognition of the FATF Forty Recommendations on Money Laundering and Eight Special Recommendations on Terrorist Financing as the international standard, and their addition, to the key standards and codes for which Reports on the Observance of Standards and Codes (ROSCs) are prepared.

I am writing now to inform you of the outcome of the discussions which took place at the FATF Plenary meeting on 9-11 October 2002 in Paris, which were highly successful and provide a firm practical basis for enhanced collaboration between the FATF and the IMF.

The FATF agreed to and endorsed the common methodology for conducting assessments of AML/CFT measures. This methodology provides a uniform basis for assessing the implementation of the FATF Recommendations by all countries, and FATF intends to apply the new methodology to all FATF mutual evaluations planned henceforth. These FATF mutual evaluations are already voluntary, co-operative and uniform, and thus consistent with the ROSC process. When the revisions to the FATF Recommendations are completed next year, the FATF will work to revise the AML/CFT methodology document accordingly, in consultation with the IMF and the World Bank. It is also important that the FATF, the IMF and the World Bank work in close co-operation to establish a common template for use in all assessments.

Additionally, the Plenary repeated its view that it will not undertake a new round of the non-cooperative countries and territories (NCCT) process during the 12 month pilot programme. The FATF reiterated its intention to continue the on-going process with respect to the countries already assessed.

ANNEX I

The collaboration with the IMF and World Bank to ensure a global program of AML/CTF assessments is an important component in FATF's overall responsibilities in the international fight against money laundering and terrorist financing. FATF looks forward to continuing to work with the IMF and World Bank during the period of the pilot program to produce quality assessments, to minimise duplication of efforts, and to jointly assess the outcome of the pilot phase. In order to strengthen co-operation between the FATF, the IMF and the World Bank, we look forward to discussing with the IMF and World Bank all aspects of information sharing regarding the assessments, including sharing copies of reports.

I can assure you that FATF is committed to this collaboration, as it is committed to its many other responsibilities, which include serving as the world-wide and acknowledged standard setter for policies to combat money laundering and the financing of terrorism; the assessment and evaluation of its members against those standards; and leading international efforts to monitor money laundering and terrorist financing techniques, methods and trends.

Please feel free to circulate this letter to the members of the Executive Board of the IMF.

I look forward to our continued successful collaboration.

Yours sincerely,

Jochen Sanio

ANNEX II

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

TABLE OF CONTENTS

Introduction

This document consists of two sections. Following this introduction, the first section consists of an overview of the assessment methodology, its background, a description of the structure of the document, and of certain conditions that are not included in the assessment criteria but that are nevertheless necessary for an effective anti-money laundering and combating the financing of terrorism ("AML/CFT") system. The second section consists of the AML/CFT assessment criteria themselves, including related descriptive material. There is also an annex that maps the relationship between the assessment criteria and the FATF Forty and Eight Special Recommendations (*to be created later*).

1. AML/CFT Assessment Methodology

1.1. Background to Methodology

The AML/CFT Methodology Document, including the assessment criteria, is designed to guide the assessment of a jurisdiction's compliance with AML/CFT standards. It is based primarily on the FATF Forty Recommendations (the FATF 40) and the FATF Eight Special Recommendations on Terrorist Financing (the FATF 8), but also includes relevant elements from United Nations Security Council Resolutions and international conventions and from supervisory/regulatory standards for the banking, insurance and securities sectors. It is also informed by the assessment experience of the FATF (from its mutual evaluations), of the Fund and Bank (in the Financial Sector Assessment Program (FSAP)) and by the Fund (in the Offshore Financial Center assessment program (OFC)).

In June 2002, the FATF Plenary instructed the FATF Secretariat to merge two earlier documents that were attached to the Bank and the Fund paper *Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT): Materials Concerning Staff Progress Towards the Development of a Comprehensive AML/CFT Methodology and Assessment Process* to constitute a draft comprehensive methodology for assessing compliance with the FATF 40+8 Recommendations.

The first document (*Fund and Bank Methodology for Assessing Legal, Institutional and Supervisory/Regulatory Aspects of Anti-Money Laundering and Combating the Financing of Terrorism)* was prepared by Bank/Fund staff in consultation with the FATF, the Basel Committee on Banking Supervision (the Basel Committee), the International Association of Insurance Supervisors ("IAIS"), the International Organization of Securities Commissions ("IOSCO") and the Egmont Group. A draft of this document, which covers the legal and institutional AML/CFT framework and AML/CFT preventive measures for the financial sector, has been used by the Fund and the Bank in conducting AML/CFT assessments as part of the FSAP and OFC initiatives, beginning in February 2002.

The second document (*Assessment of Implementation of Legal and Institutional Elements Outside of the Supervisory or Regulatory Framework)* was prepared by an FATF Working Group in consultation with the Egmont Group. This draft document contained assessment criteria relating to the implementation of penal and repressive measures that are required for a comprehensive AML/CFT regime.

1.2. The Structure of the Methodology Document

An effective AML/CFT system requires an adequate legal and institutional framework, which should include: (i) laws that create AML/CFT offences and other penal measures, and that impose the required obligations on financial institutions (ii) an appropriate institutional or administrative framework, and (iii) laws that provide competent authorities with the necessary duties, powers and sanctions, including the ability to co-operate internationally. It is also essential that the competent authorities ensure that the whole system is effectively implemented.

Section 2 of this methodology is therefore divided into three sections. There are two principal sections (2.1 & 2.2) that contain assessable criteria. Section 2.1 deals with criminal justice measures, FIUs and international co-operation, and section 2.2 covers preventive measures for financial institutions. The first part of section 2.2 contains assessment criteria that are based on the FATF 40 + 8, and which are applicable to all financial institutions. This is followed by three sub-parts that contain sector –specific measures for the banking, insurance and securities sectors, where the criteria are based on standards applicable to AML/CFT that have been issued by the Basel Committee, IAIS or IOSCO. Finally, section 2.3 seeks information on any measures that a jurisdiction may have adopted regarding monitoring or reporting of large currency or cross-border transactions.

Section 2.1: Criminal Justice Measures, ~~the FIU~~ and International Co-operation

This section is drawn mainly from the FATF 40+8, but also relies on relevant international conventions and U.N. Security Council Resolutions. The assessment criteria are set out in five sub-sections, covering I (Criminalisation of ML and FT), II (Confiscation), III (The FIU and processes for receiving, analysing, and disseminating financial information and other intelligence at both domestic and international levels), IV (Law enforcement and prosecution authorities, powers and duties), and V (International co-operation).

Section 2.2: Preventive measures for financial institutions

Section 2.2 applies to the banking, insurance, and securities sectors as well as other financial sectors that are vulnerable to ML and FT. These other categories of financial institutions should include all financial institutions as covered by the FATF 40+8, including in particular, bureaux de change (foreign exchange offices) and money remittance or transfer companies. The assessment criteria are set out in nine sub-sections, covering: I (General Framework), II (Customer identification), III (Ongoing monitoring of accounts and transactions), IV (Record keeping), V (Suspicious transactions reporting), VI (Internal controls, Compliance and Audit), VII (Integrity standards), VIII (Enforcement powers and sanctions), and IX (Co-operation between supervisors and other competent authorities).

Section 2.2.1 contains the criteria for assessing the legal and institutional elements that are required for all financial institutions. For each of these criteria it is also necessary to assess whether those measures have been effectively implemented. Sections 2.2.2, 2.2.3 and 2.2.4 contain additional sector-specific criteria for the banking, insurance, and securities sectors, which has been provided by the relevant standard setters (the Basel Committee, IAIS, and IOSCO) and which are based on standards they have issued.

Section 2.3: Monitoring or reporting of large currency or cross-border transactions

This section is based on FATF Recommendations ~~22-24~~,22-23, which although discretionary Recommendations, do form an integral part of the AML/CFT systems in a number of jurisdictions. The section therefore seeks information from each jurisdiction on any

measures that it may have taken concerning the monitoring or reporting of large currency or cross-border transactions, and the use of cash. Although the section does not contain assessable criteria, assessors should review any measures that have been taken, and should note any significant deficiencies.

1.3. Other conditions necessary for an effective AML/CFT system

A truly effective AML/CFT system requires that other conditions not covered by the AML/CFT assessment criteria also be in place. These include sound and sustainable financial sector policies and a well-developed public sector infrastructure. In particular, effectiveness depends on a proper culture of deterrence shared and reinforced by government, financial institutions, other providers of financial services, industry trade groups, and self-regulatory organisations (SROs). The infrastructure requires ethical and professional lawyers, examiners, accountants, auditors, police officers, prosecutors, and judges, etc., and a reasonably efficient court system whose decisions are enforceable. An essential aspect of assessing the adequacy of these conditions is the existence of a system for ensuring the ethical and professional behaviour on the part of examiners, accountants and auditors, and lawyers, including the existence of codes of conduct and good practices, as well as methods to ensure compliance such as registration, licensing, and supervisory bodies.

Weaknesses or shortcomings in these areas may significantly impair the implementation of an effective AML/CFT framework. Although the AML/CFT assessment criteria do not cover these conditions, apparent major weaknesses or shortcomings identified should be noted in the detailed assessment report.

2. The AML/CFT Assessment Criteria

Assessment and Compliance

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

Assessors should be aware that the legislative, institutional and supervisory framework for AML/CFT may differ substantially from one jurisdiction to the next. Provided the relevant international standards for combating ML and FT are met, it is acceptable that jurisdictions implement the standards in a manner consistent with their national legislative and institutional systems. Consistent with the modalities for assessments under the ROSC framework, account should be taken of each jurisdiction's stage of economic development, its range of administrative capacities, and different cultural and legal conditions. Moreover, the report should provide the context for the assessment, and make note of any progress that has been or is being made in implementing the international standards and the criteria in this methodology.

A requirement is considered **compliant** whenever it is fully observed. A requirement is considered **largely compliant** whenever only discrete and non-systemic shortcomings are observed which do not raise major concerns and when corrective actions to achieve full observance with the requirement are readily identified and have been scheduled within a reasonable period of time. A requirement is considered **materially non-compliant** whenever discrete or non-systemic shortcomings are observed that are not addressed, or whenever numerous or systemic shortcomings are observed and corrective actions are identified and have been scheduled within a reasonable period of time. A requirement is considered **non-compliant** whenever the jurisdiction has not addressed the issue or has addressed it in a manner that cannot reasonably lead to substantial observance. A requirement is considered not applicable whenever, in the view of the assessor, the requirement does not apply, given the structural, legal and institutional features of a jurisdiction. Assessors should review whether the laws meet the appropriate standard and whether there is adequate capacity and implementation of the laws. Laws that impose preventive AML/CFT requirements upon the banking, insurance, and securities sectors are generally implemented and enforced through the supervisory process. For other types of financial institutions, it will vary from jurisdiction to jurisdiction as to whether these laws and obligations are implemented and enforced through a regulatory or supervisory framework, or by other means.

Definitions

Financial Institutions consists of banks, insurance entities, and securities firms (which are subject to prudential regulation under Basel Committee, IAIS, and IOSCO supervisory principles) as well as other financial institutions covered by the FATF Forty

Recommendations, including bureaux de change (foreign exchange offices) and money remittance or transfer companies[1].

The Financial Intelligence Unit (FIU)[2] is a central, national agency responsible for receiving (and, as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information (i) concerning suspected proceeds of crime; or (ii) required by national legislation or regulation, in order to counter money laundering.

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

Law includes legislation, decree, regulation, or other rule that is in force, is mandatory, and for which there are sanctions for non-compliance.

Supervisor/regulator refers to the agency or body that is responsible for oversighting compliance by financial institutions with AML/CFT requirements and obligations and/or the prudential supervision of financial institutions. In some jurisdictions this may be the agency/body responsible for the prudential supervision of such institutions, while in others it could be another competent authority, such as the FIU.

Criteria to be assessed are numbered sequentially. In some cases elaboration (indented below the criteria) is provided in order to assist in identifying important aspects of the assessment of the criteria. *Criteria that involve the assessment of* ~~law enforcement or prosecutorial elements of an AML/CFT system i.e. the implementation (either~~*either the capacity to implement or the effectiveness of implementation*~~)~~ *of criminal justice requirements are set out in italics.*

2.1. CRIMINAL JUSTICE MEASURES AND INTERNATIONAL CO-OPERATION

I. Criminalisation of ML and FT

1. ~~1.~~ The jurisdiction should have ratified and fully implemented the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988 (Vienna Convention), the UN International Convention for the Suppression of the Financing of Terrorism 1999, and the UN Convention Against Transnational Organized Crime 2000 (Palermo Convention), as well as other regional AML/CFT conventions (e.g. the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime), where applicable. Countries should also immediately implement the United Nations resolutions relating to ~~The jurisdiction should have fully implemented the provisions of these conventions relevant to AML/CFT through its domestic law~~the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373. (see FATF 1, 35, I).

[1] This includes all persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network (see FATF VI).

[2] Egmont Group definition of an FIU.

2. Each jurisdiction should criminalise money laundering on the basis of the Palermo and Vienna Conventions (see FATF 4).

2.1. The offence of ML ~~should~~may extend not only to those persons who have committed ML, but also to persons who have committed both the laundering and the predicate offence.

2.2. It should not be necessary that a person be convicted of a predicate offence to establish that assets were the proceeds of a predicate offence and to convict any person of laundering such proceeds.

2.3. Predicate offences for ML should extend to all serious offences, including drug trafficking and FT offences. (see FATF 4, II) It is possible to identify ML predicate offences by list or generically, including by length of penalty.

2.4. The offence of ML should extend to any type of property that directly or indirectly represents the proceeds of crime.

2.5. The predicate offences for ML should extend to conduct that occurred in another country, and which would have constituted a predicate offence had it occurred domestically.

3. FT should be criminalised on the basis of the Convention for the Suppression of the Financing of Terrorism (see FATF II).

3.1. The FT offence should also apply when the terrorists or terrorist organisations are located in another jurisdiction or when the terrorist acts take place in another jurisdiction (see FATF II).

4. The offences of ML and FT should apply at least to those individuals or legal entities that knowingly engage in ML or FT activity. Laws should provide that the intentional element of the offences of ML and FT may be inferred from objective factual circumstances. ~~If permissible under the jurisdiction's legal system, theoffences of ML and FT should extend to those who "should have known" that the assets were processed for the purpose of ML or FT~~ (see FATF 5).

4.1. If permissible under the jurisdiction's legal system, the offences of ML and FT should extend to legal entities (e.g., companies, foundations) (see FATF 6).

5. Laws should provide for effective, proportionate and dissuasive criminal, civil or administrative sanctions for ML and FT.

6. ~~6. *The necessary legal*~~*Legal means and resources should be* ~~*established*~~*adequate* *to enable an effective implementation of ML and FT laws.*

II. Confiscation of proceeds of crime or property used to finance terrorism

7. Laws should provide for the confiscation of laundered property[3], proceeds from, and instrumentalities used in or intended for use in the commission of any ML or predicate offence, and property of corresponding value. Laws should provide for the confiscation of property that is the proceeds of, or used in, or intended or allocated for use in FT. (see FATF 7, III).

7.1. Laws and other measures should provide for the freezing and/or seizing of property that is, or may become, subject to confiscation. Such laws or measures may provide that the initial application to freeze or seize property can be made on an ex parte basis.

7.2. If permissible under the jurisdiction's legal system, ~~and in accordance with the Palermo Convention, laws should~~States should consider laws that provide for the confiscation of 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).

7.3 Laws should provide for confiscation of property of corresponding value, in the event that property that is subject to confiscation is not available (see FATF 7, III).

7.4 If permissible under the jurisdiction's legal system, jurisdictions should consider laws which allow for confiscation without conviction (*civil forfeiture*),~~or which allow the onus of proof to be reversed in certain situations regarding proof of the legal or illegal origin of property,~~ in addition to the system of confiscation triggered by a criminal conviction.

8. 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 or used for FT (see FATF 7, III).

9. Laws should provide protections for the rights of bona fide third parties. Such protections should be consistent with the standards provided in the Palermo Convention and Strasbourg Convention, where applicable (see FATF 7).

10. In addition to confiscation and criminal sanctions, if permissible under the jurisdiction's legal system, there should be authority to void contracts or render them unenforceable where parties to the contract knew or should have known that as a result of the contract the authorities would be prejudiced in their ability to recover financial claims resulting from the operation of AML/CFT laws (see FATF 7).

11. Authorities should keep statistics on the amounts of property frozen, seized, and confiscated relating to ML, the predicate offences and FT (see FATF 7, 38).

12. Training should be provided to administrative, investigative, prosecutorial, and judicial authorities for enforcing laws related to the freezing, seizure, and confiscation of property.

---

[3] Property should include property that is income or profit derived from the proceeds of crime.

13. Laws and other measures should provide for freezing without delay of funds or other property of terrorists, those who finance terrorism and terrorist organisations, in accordance with the United Nations resolutions relating to the prevention and suppression of FT (e.g., U.N.SCRs 1267, 1269, 1390) (see FATF III)

13.1 Authorities should keep statistics on the amounts of property frozen relating to FT and the number of individuals or entities whose property have been frozen.

14. Competent authorities should have the power to identify and freeze the property of suspected terrorists, those who finance terrorism and terrorist organisations, ~~whose~~even where the names ~~may~~of such persons do not appear on the list(s) maintained by the relevant committees of the U.N. Security Council.

15. If permissible under the jurisdiction's legal system, the jurisdiction should consider establishing an asset forfeiture fund into which all or a portion of confiscated property will be deposited and will be used in the management of seized and confiscated property, as well as for law enforcement, health, education or other appropriate purposes (see Interpretative Note to FATF 38).

16. If permissible under the jurisdiction's legal system, the jurisdiction should consider asset sharing mechanisms to enable it to share confiscated property with other jurisdictions, particularly when confiscation is directly or indirectly the result of co-ordinated law enforcement actions. Unless otherwise agreed, such reciprocal sharing arrangements should not impose conditions on jurisdictions receiving the shared property. (see FATF 38, Interpretative Note to FATF 38).

III. The FIU and processes for receiving, analysing, and disseminating financial information and other intelligence at the domestic and international levels

17. An FIU that meets the Egmont Group definition should be established for receiving, analysing, and disseminating disclosures of financial information and other relevant information and intelligence concerning suspected ML or FT activities (see Egmont Statement of Purpose).

17.1 Reporting parties should be required to send all STR[4] and currency transaction reports (where a jurisdiction requires reports to be filed for large currency transactions) to the FIU.

17.2 The FIU or another competent authority should issue guidelines for the identification of complex and unusual transactions or patterns or transactions, and suspicious patterns of behaviour (see FATF 14, 28).

[4] For jurisdictions that have a system of reporting of unusual transactions, references to "suspicious transaction reports" should be read as including unusual transaction reports.

17.3 The reporting procedures should be prescribed by law. Financial institutions and other reporting parties should be provided with guidance regarding the manner of reporting, including the specification of reporting forms.

18. The FIU or other competent authorities should be authorised to obtain from reporting parties, either directly or through another competent authority, additional documentation needed to assist in its analysis of financial transactions.

19. The FIU, either directly or through other competent authorities, should have access to financial, administrative and/or law enforcement information, on a timely basis, to enable it to adequately undertake its responsibilities.

20. The FIU or another competent authority should be authorised to order sanctions or penalties (including meaningful fines and/or license suspensions) against reporting parties for failure to comply with their reporting obligations.

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

22. The FIU should be authorised to share financial information and other relevant intelligence with its foreign counterpart FIUs, either on its own initiative or upon request (see Egmont Principles for Information Exchange).

22.1 There should be adequate safeguards, including confidentiality, to ensure that this exchange of information is consistent with national laws and international agreed principles on privacy and data protection (see FATF 32).

23. ~~FIUs~~Where applicable, FIUs or other competent authorities should keep statistics on the number of:

- *STRs received by the FIU or other competent authorities as well as the number of STRs analysed and disseminated;*
- *STRs resulting in investigation, prosecution, or convictions;*
- *Requests for assistance received by the FIU or other competent authorities, from both domestic and foreign authorities, as well as the number of responses provided to the requests received;*
- *Spontaneous referrals made by the FIU or other competent authorities to both domestic and foreign authorities; and*
- *If the jurisdiction requires the reporting of large currency transactions, statistics should be kept on the number of reports filed.*

24. The FIU should be adequately structured, funded, staffed, and provided with sufficient technical and other resources to fully perform its authorised functions.

24.1 The FIU should have an organisational structure sufficient to ensure that its functions are properly executed.

24.2 The FIU can be established either as an independent governmental authority or within an existing authority or authorities, but in either case it should have sufficient independence and autonomy to ensure that (i) it is free from unauthorized outside influence or interference in its functions and decisions; and (ii) that information and

intelligence held by it will be securely protected and disseminated only in accordance with the law.

24.3 The FIU should publish periodic reports, including statistics, typologies and trends regarding its activities.

~~25. The FIU, including its employees, should have adequate legal protection against proceedings arising from the bona fide execution of their duties.~~

IV. Law enforcement and prosecution authorities, powers and duties

~~26.~~25. *Designated law enforcement authorities should have responsibility for ensuring that ML and FT offences are properly investigated.*

~~27.~~26. There should be an adequate legal basis for the use of a wide range of investigative techniques, ~~including~~such as controlled delivery,~~lawful interception provisions,~~ undercover operations, etc.

~~27.1~~26.1 Where permitted, the use of such techniques should be encouraged when conducting investigations of ML, FT, and the predicate offences (FATF 36 and Interpretative Note to FATF 36).

~~28.~~27. Law enforcement authorities should be able to compel production of bank account records, financial transaction records, customer identification records, and other records maintained by financial institutions and other entities or persons, through lawful process (for example, subpoenas, summonses, search and seizure warrants, or court orders could be used), as necessary, to conduct investigations of ML, FT, and predicate offences. (see FATF 37).

~~29.~~28. *Where necessary, appropriate mechanisms (such as a "task force") should be created to ensure adequate co-operation and information sharing among the different government agencies that may be involved in investigations of ML, FT, and predicate offences (e.g., police, customs, FIU and/or other competent authorities).*

~~30.~~29. *Law enforcement and prosecution agencies that are authorised to investigate and prosecute ML and FT should be adequately structured, funded, staffed, and provided with sufficient technical and other resources to fully perform these functions.*

~~31.~~30. *Authorities should keep statistics of the number of ML and FT investigations, prosecutions, and convictions, including statistics of investigations initiated on the basis of STRs, and as a result of "on the street" or predicate offence investigations. Authorities should also keep statistics on any criminal, civil, or administrative sanctions applied.*

~~32.~~31. *Typologies and trends should be reviewed on a regular, interagency basis, and information should be disseminated to law enforcement personnel on current ML and FT methods and techniques.*

~~33.~~32. *Adequate training should be provided to administrative, investigative, prosecutorial, and judicial authorities for enforcing laws to combat ML and FT, in particular concerning the scope of predicate offences, ML and FT typologies, techniques to investigate and prosecute these offences, and 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.*

~~33.1~~32.1 *Jurisdictions should consider providing special training and/or certification for financial investigators for, inter alia, investigations of ML, FT, and the predicate offences.*

~~34~~33. *Adequate efforts should be made to address problems encountered by the authorities in achieving successful investigations, prosecutions, and convictions, and in freezing, seizing and confiscating the proceeds of crime or property to be used to finance terrorism.*

V. International Co-operation

~~35.~~34. There should be laws and procedures ~~for~~allowing the provision of the widest possible range of mutual legal assistance in AML/CFT ~~law enforcement matters regarding~~matters, whether requiring the use of compulsory measures or not, and including the production of records by financial institutions and other persons, the search of persons and premises, seizure and obtaining of evidence for use in AML/CFT investigations and prosecutions and in related actions in foreign jurisdictions (see FATF 3, 32, 34, 36, 37, 38, 40, I and V).

~~35.1~~34.1 There should be appropriate laws and procedures to provide effective mutual legal assistance in AML/CFT investigations or proceedings where the requesting jurisdiction is seeking: (i) the production or seizure of information, documents, or evidence (including financial records) from financial institutions, other entities, or natural persons; searches of financial institutions, other entities, and domiciles; (ii) the taking of witnesses' statements; and (iii) 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, ~~or~~and assets of corresponding value (see FATF ~~33,~~34, 37, 38, V).

~~35.2~~34.2 Assistance should be provided in investigations and proceedings where persons have committed both the money laundering and the predicate ~~offense~~offence as well as in investigations and proceedings where persons have committed ~~laundering only (see FATF 3).~~the money laundering offence only (see FATF 33).

~~37.~~36. International co-operation should be supported~~, such as~~ through the use of conventions, treaties, agreements or arrangements, whether bilateral or multilateral~~mutual legal assistance treaties or other formal arrangements, but also through informal mechanisms~~ (see FATF 3, ~~33).~~34).

~~38.~~37. There should be arrangements in place for law enforcement authorities to exchange information regarding the subjects of investigations with their international counterparts, based on agreements in force and by other mechanisms for co-operation. *The authorities should record the number, source, and purpose of the request for such information exchange, as well as its resolution* (see FATF 34, V).

~~39.~~38. Co-operative investigations, including controlled delivery, with other countries' appropriate competent authorities should be authorised, provided that adequate safeguards are in place e.g. a need for judicial authorisation (see FATF 3, 36).

~~40.~~39. *There should be arrangements for co-ordinating seizure and forfeiture actions, including, where permissible, authorising~~for~~ the sharing of confiscated assets with other*

countries when confiscation is directly or indirectly a result of co-ordinated law enforcement actions (see FATF 38, 39).

~~41.~~40. There should be laws and procedures to extradite individuals charged with a ML or FT offence or related offences ~~or to permit prosecution domestically when not extraditable (see FATF 3, 39, 40, V).~~(see FATF 3, 40, V).

40.1 Where a jurisdiction does not extradite its own nationals pursuant to extradition requests, that jurisdiction should, at the request of the jurisdiction seeking extradition, and in accordance with the general principles relating to mutual assistance, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request.

41. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals. (FATF V).

42. Relevant authorities should be provided adequate financial, human or technical resources to ensure adequate oversight and to conduct investigations and to respond promptly and fully to requests for assistance received from other countries.

2.2. PREVENTIVE MEASURES FOR FINANCIAL INSTITUTIONS

2.2.1. All financial institutions - the legal and institutional framework and its effective implementation

In order to assess compliance with the following criteria (43-66), assessors must verify that:

~~that~~(a) the laws and institutional framework are in place; and
~~place. Assessors must also verify that~~(b) there are effective supervisory/regulatory measures in force that ensure that those criteria are being properly and effectively implemented by all financial institutions.

Both aspects are of equal importance.

I. General Framework

43. ~~No~~Jurisdictions should ensure that no confidentiality or secrecy law or ~~agreement should prevent~~agreement, or any other law, will inhibit the implementation of the criteria set out in this methodology (FATF 2).

~~44 Laws should require designation of a supervisor/regulator~~44. Jurisdictions should designate competent authorities to ensure effective implementation of~~AML/CFT policies, consistent with~~ the FATF 40+8 Recommendations, by all financial institutions.

II. Customer identification

45. Financial institutions should be prohibited from keeping anonymous accounts or accounts in fictitious names. ~~Numbered accounts should only be permitted if the financial institution has properly identified the customer in accordance with these criteria, and the customer identification records are available to the AML/CFT complianceofficer and other appropriate staff~~ (see FATF 10).

46. Financial institutions should be required to identify their customers on the basis of an official or other identifying document, and to record their identity,~~of their customers~~ when establishing business relations, and to identify and record the identity of their occasional customers when performing transactions over a specified threshold and to renew identification when doubts appear as to their identity in the course of their business relationship (see FATF 10).

46.1 If the customer is a legal entity, financial institutions should~~be required~~ adequately~~to~~ verify its legal existence and structure, including information concerning: (a) the customer's name, legal form, address, directors; (b) whenever it is necessary, in order to know the true identity of the customer, request information from the ~~directors, and~~customer concerning the principal owners ~~and/or beneficiaries, and~~and beneficiaries; and (c) provisions regulating the power to bind the ~~entity,~~entity; and to verify that any person purporting to act on behalf of the customer is so authorised, and identify those persons (see FATF 10, 11).

46.2 Numbered accounts should only be permitted if the financial institution has properly identified the customer in accordance with these criteria, and the customer

identification records are available to the AML/CFT compliance officer, other appropriate staff and the supervisor.

47. -Financial institutions should be required to take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf (see FATF 11).

48. Financial institutions, including money remitters, should be required to include accurate and meaningful originator information on funds transfers and related messages~~on wire transfers~~ that should remain with the transfer or related message through the payment chain. Originator information should include name, address, and account number (when being transferred from an account) (see FATF VII, and its Interpretative Note once this is adopted by the FATF).

III. Ongoing monitoring of accounts and transactions

49. 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, to examine as far as possible the background and purpose of such transactions, to set forth their findings in writing, and to keep such findings available for competent authorities (see FATF 14).

50. Financial institutions should be required to give special attention to business relations and transactions with persons (including legal entities and other financial institutions) in jurisdictions that do not have adequate systems in place to prevent or deter ML or FT. 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 such as supervisors, law enforcement agencies and the FIU, and auditors (see FATF 21).

50.1. There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML or CFT systems of other countries (see FATF 21, 28).

51. Financial institutions should be required to give enhanced scrutiny to wire transfers that do not contain complete originator information (see FATF VII).

IV. Record keeping

52. Financial institutions should be required in all cases to maintain records on customer identity (including where possible, copies of the official or other identifying document) 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 upon proper authority). Such documents should be available for inspection by a competent authority (see FATF 12).

53. Financial institutions should be required to maintain all necessary records concerning customer transactions, and accounts, for at least five years following completion of the transaction (or longer if requested by a competent authority upon proper authority), regardless of whether the account or business relationship is terminated and these documents should be available to a competent authority (see FATF 12).

53.1 Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal behaviour. Records should include the customer's ~~(or~~(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.

54. Financial institutions should be required to ensure that customer and transaction records and information are available to domestic competent authorities for AML/CFT investigations and prosecutions (see FATF 12).

V. Suspicious transactions reporting

55. If a financial institution suspects that assets involved in a transaction either stem from a criminal activity or are linked or related to, or are to be used to finance terrorism, the financial institution should be required to report promptly its suspicions to the FIU in the form of a "suspicious transaction report" ("STR") (see FATF 15, IV).

55.1 Financial institutions should be required to have clear procedures, communicated to all personnel, for reporting suspicious transactions~~ to: (i) the AML/CFT compliance officer; and then (ii) the FIU~~.

55.2. The FIU or other competent authorities should establish guidelines to assist financial institutions in detecting patterns of suspicious ~~patterns of behaviour~~financial activity by their customers. Such guidelines should also include: (i) a description of ML and FT techniques, methods and trends; (ii) an explanation of the AML/CFT laws and requirements that apply; and guidance on how a financial institution could comply with those laws and requirements (see FATF 28).

56. Financial institutions (including any directors, officers, and employees) should be protected from any liability for breach of any restriction on disclosure of information in the course of making available findings or reporting suspicions in good faith to the FIU (see FATF 16).

57. Financial institutions (including any directors, officers and employees) should be prohibited from warning ("tipping off") their customers when information relating to them is reported to competent authorities. Directors, officers and employees should observe the instructions from the FIU or other competent authority to the extent that they carry out further investigation or review (see FATF 17, 18).

VI. Internal controls, Compliance and Audit

~~58. Laws should require that financial institutions ensure that their foreign branches and subsidiaries observe appropriate AML/CFT measures consistent with the home jurisdiction requirements and that financial institutions inform their home jurisdiction supervisor/regulator when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures of the home jurisdiction. Where the AML/CFT requirements in a host jurisdiction are of a higher standard than in the home jurisdiction, then the foreign branch or subsidiary should apply the higher standard (see FATF 20).~~

~~59.~~58. Financial institutions should be required to establish and maintain internal procedures to prevent their institutions from being used for ML or FT purposes. In particular, financial institutions should be required to establish AML/CFT programs that include internal procedures and policies (such as customer acceptance policies), ongoing employee training, and an audit function to test the system, to ensure adequate compliance with these programs (see FATF 19).

~~59.1~~58.1 In relation to ongoing training, financial institutions should be required 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 customer identification and due diligence, and suspicious transaction reporting. (see FATF 19)

59. Financial institutions should be required to designate an AML/CFT compliance officer at management level (see FATF 19).

~~61.~~60. Financial institutions should be required to~~be required to~~ put in place adequate screening procedures to ensure high standards when hiring employees (see FATF 19).

~~60. Financial institutions should be required to designate an AML/CFT compliance officer at management level (see FATF 19).~~

61. Financial institutions should ~~be required to put in place adequate screening procedures to ensure high standards when hiring employees (see FATF 19).~~
ensure that their foreign branches and subsidiaries observe appropriate AML/CFT measures consistent with the home jurisdiction requirements, to the extent that local laws and regulations permit. Financial institutions should inform their home jurisdiction supervisor/regulator when a foreign branch or subsidiary is unable to observe the appropriate AML/CFT measures of the home jurisdiction. (see FATF 20).

61.1 Where the minimum AML/CFT requirements of the home and host jurisdictions differ, branches and subsidiaries in host jurisdictions should be required to apply the higher standard.

VII. Integrity standards

62. Criminals should be prohibited from holding or controlling a significant investment in a financial institution, or from holding any qualified management functions therein, including in the executive or supervisory boards, councils, etc (see FATF 29).

62.1 Laws ~~should require registration, authorisation, and/or licensing of financial institutions~~or regulatory measures should be adopted to prevent, inter alia, criminals from gaining control of or holding a significant investment interest or~~any~~ management function in a financial institution.

62.2 ~~Laws should require that directors~~Directors and senior management of financial institutions ~~are~~subject to prudential supervision should be evaluated as to expertise and integrity. Criteria for qualification should include: (i) skills and experience in relevant financial operations commensurate with the intended activities of the financial

institution, and (ii) no record of criminal activities or adverse regulatory judgments that would make the person unfit to be a director or senior manager of that institution.

63. There should be measures to prevent unlawful use of entities identified as vulnerable to use as conduits for criminal proceeds or FT, such as shell corporations or charitable or not-for-profit organisations (see FATF 25, VIII).

VIII. Enforcement powers and sanctions

64. Laws should provide the supervisor or other competent authority with adequate powers of enforcement and sanction against financial institutions, and their directors or senior management for failure to comply with or properly implement the criteria set out in this methodology, including the power to withdraw or suspend ~~their license (see FATF 26).~~the institution's license.

IX. Co-operation between supervisors and other competent authorities

65. The supervisor/regulator should be adequately structured, funded, staffed, and provided with sufficient technical and other resources, including specialised expertise on AML/CFT, to fully perform its authorised AML/CFT functions.

66. ~~Supervisors~~The supervisor/regulator should co-operate, spontaneously or upon request, with other domestic competent authorities including the lending of expertise with respect to AML/CFT analysis, investigations, and prosecutions (see FATF 26).

67. There should be laws and procedures allowing the provision of the widest possible range of international co-operation between supervisors/regulators, consistent with their respective mandates. There should also be clear gateways in place for exchange of information relating to ML and FT and there should not be unduly restrictive conditions on such exchange.

Specific criteria for the banking, securities and insurance sectors

The core assessment criteria for the legal and institutional framework of an AML/CFT system for financial institutions are set out in ~~Part B1~~section 2.2.1 above. These criteria are largely drawn from the FATF Recommendations, and are broadly applicable to all financial institutions. However, for the banking, insurance, and securities sectors, the AML/CFT elements and assessment criteria also draw from the supervisory and regulatory principles issued by the Basel Committee (section 2.2.2 - sector-specific criteria for the banking sector); the IAIS (section 2.2.3 - sector specific criteria for the insurance sector); and IOSCO (section 2.2.4 - sector specific criteria for the securities sector).[5] These additional criteria are set out below.

As with section 2.2.1 above, assessors must not only check that all the legal and institutional requirements in sections 2.2.2, 2.2.3 and 2.2.4 have been imposed or exist, but must also verify that there are effective supervisory/regulatory measures in force that ensure

[5] It should be understood that the sector-specific information in the AML/CFT methodology will not replace any of the individual core principles of the standards issued by the Basel Committee, IAIS and IOSCO.

that those criteria are being properly and effectively implemented in the banking, insurance and securities sectors.

Assessors should pay particular attention when there are increased risks of ML or FT due to factors such as a high usage of cash or cash equivalents in a jurisdiction or financial sector; or a the prevalence of financial products that can be more vulnerable to ML e.g., single premium life insurance policies.

2.2.2. Banking sector: sector-specific criteria

The Basel Committee's Core Principles for Effective Banking Supervision (BCP) set out the necessary foundations of a sound supervisory system. The following principles are relevant to AML/CFT: BCP1 on arrangements for sharing information between supervisors; BCP3-5 on licensing and structure; BCP14 on adequate internal controls; BCP15 on adequate policies to prevent use by criminal elements; and BCP23-25 on co-operation between home and host supervisors. In October 2001, the Basel Committee issued detailed ~~AML/CFT~~prudential recommendations in its "Customer due diligence for banks" (CDD) paper.~~paper.~~

~~The specific criteria for banks~~The banking sector specific criteria in this section are drawn extensively from ~~this~~the CDD paper and should be interpreted with reference to the corresponding paragraphs in ~~this paper.~~that paper. These criteria have been endorsed by the Basel Committee. Supervisors may use a range of methods to enforce criteria 67 to 91, such as through legislation and regulations, or through guidance or codes of practice which banks should follow. In assessing compliance with these criteria, assessors should verify that supervisors monitor their effective implementation by banks in their jurisdictions.

The specific criteria for the banking sector are in addition to the core assessment criteria based on the FATF Recommendations. There are no additional criteria for sections I (General framework), V (Suspicious transactions reporting), VII (Integrity standards).

II. Customer identification

~~67.~~68. Banks should~~be required to~~ have in place graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers (CDD 20).

~~68.~~69. Banks should~~be required to~~ take decisions to enter into business relationships with higher risk customers at the senior management level (CDD 20).

~~69.~~70. Banks should~~be required to~~ identify the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners); the beneficiaries of transactions conducted by professional intermediaries; and any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank (CDD 21).

~~70.~~71. Banks should~~be required to~~ establish a systematic procedure for identifying customers and should not establish a banking relationship until the identity of a customer has been satisfactorily verified. Banks should be required to keep customer identification information up-to-date and relevant by undertaking regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, when there is a material change in the way that the account is

operated, or when the bank becomes aware that it lacks sufficient information about an existing customer (CDD 22, 24).

~~71.~~72. Banks should~~be required to~~ pay special attention to non-resident customers and ~~document~~understand the reasons for which the customer has chosen to open an account in the foreign country (CDD 23).

~~72.~~73. Banks should~~be required to~~ apply enhanced due diligence to private banking operations (CDD 25).

~~73.~~74. Banks should~~be required to~~ apply enhanced diligence procedures to a customer, if it has any reason to believe that the customer is being refused banking facilities by another bank (CDD 29).

~~74.~~75. When an account has been opened, but problems of verification arise in the banking relationship which cannot be resolved, banks should~~be required to~~ close the account and return the monies to the source from which they were received, subject to any national legislation concerning handling of suspicious transactions (CDD 28).

~~75. There should be guidance to assist banks in the area of customer identification (CDD 27).~~

76. Where the customer is a trust, banks should~~be required to~~ obtain information about the trustees, settlors/grantors and beneficiaries (CDD 32).

77. Where the customer is a corporate vehicle,~~ which can beused to operate anonymous accounts,~~ banks should be required to understand and document the structure of the company, determine the source of funds and identify the beneficial owners and those who have control over the funds~~.~~, to prevent the corporate vehicle being ~~Special care needs to be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form (CDD 33, 34).~~used to operate anonymous accounts. Special care needs to be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form (CDD 33, 34).

78. When banks use introducers, the ultimate responsibility for knowing customers always lies with the bank. Banks should~~be required to~~ use the following conditions when determining whether it can rely on introducers:

- The introducer complies with the minimum customer due diligence standards required of banks;
- The customer due diligence procedures of the introducer are as rigorous as those which the bank would have conducted itself for the customer;
- The bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- The bank must reach agreement with the introducer that it will be permitted the right to verify the due diligence undertaken by the introducer; and
- All relevant identification data and other documentation pertaining to the customer's identity are immediately submitted by the introducer to the bank (CDD 36).

79. Banks should~~be required to~~ identify the beneficial owners of client accounts opened by professional intermediaries; exceptions may apply only to co-mingled accounts in circumstances clearly set out by regulations or supervisory guidance, subject to following conditions:

- The intermediary is subject to the same regulatory and money laundering legislation and procedures, and the same customer due diligence standards in respect of its client base, as the bank;
- The bank is able to establish that the intermediary has engaged in a sound due diligence process;
- The intermediary is able to allocate the assets in the pooled accounts to the relevant beneficiaries; and
- The intermediary is able to furnish the required information on beneficiaries to the bank (CDD 39, 40).

80. Banks should~~be required to~~ have policy and procedures for handling banking relationships with politically exposed persons (PEPs) that cover:

- Identification of a politically exposed person among new or existing customers;
- Identification of persons or companies related to them;
- Verification of the source of funds prior to account opening; and
- Senior management approval for establishing banking relationships with PEPs (CDD 41, 44, 54).

81. Banks should~~be required~~ not~~to~~ accept or maintain a business relationship if the bank knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the bank has under criminal law or other laws or regulations (CDD 43).

82. Banks should~~be required to~~ apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview and there must be specific and adequate measures to mitigate the higher~~risk. Examples of measures to mitigate risk include: certification of documents presented;requisition of additional documents to complement those which are required for face-to-face customers; independent contact with the customer by the bank; third party introduction; or requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer duediligence standards~~ (CDD 48).

83. Banks should~~be required to~~ have policies and procedures regarding the opening of correspondent accounts. The policy and procedures should at the minimum require the bank:

- To fully understand and document the nature of the respondent bank's management and business;
- To ascertain that the respondent bank has effective customer acceptance and KYC policies and is effectively supervised;

- To identify and monitor the use of correspondent accounts that may be used as payable-through accounts; and
- Not to enter into or continue a correspondent relationship with a bank incorporated in a jurisdiction in which it has no physical presence (i.e. meaningful mind and management)[6] and which is unaffiliated with a regulated financial group (i.e. shell banks) (CDD 50, 52).

III. On-going monitoring of accounts and transactions

84. Banks should be ~~required to have systems in place~~able to aggregate and monitor significant balances and activity in customer accounts on a fully consolidated worldwide basis, regardless of whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis (CDD 16).

85. Banks should~~be required to~~ have systems in place to detect unusual or suspicious patterns of activities in all accounts, such as 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 (CDD 53).

86. Banks should~~be required to~~ conduct intensified monitoring for higher risk accounts (CDD 54).

87. Banks should~~be required to~~ pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified as being "non-cooperative" in the fight against anti-money laundering. Banks should also be required to pay particular attention to transactions involving such jurisdictions (CDD 51, 62).

IV. Record keeping

88. Banks should~~be required to~~ develop clear standards on what records must be kept on customer identification and individual transactions and their retention period (CDD 26).

VI. Internal controls, compliance and audit

89. Banks should~~be required to~~ establish procedures, and to allocate responsibilities to ensure that KYC policies and procedures are managed effectively and are in line with local supervisory practice (CDD 55).

90. Banks should~~be required to~~ have in place an adequately resourced compliance function, which provides independent evaluation of the bank's own policies and procedures and is responsible for the ongoing monitoring of staff performance through sample testing of compliance and for reporting to senior management or the Board of Directors in case of failures in KYC procedures (CDD 56, 57).

91. Banks and banking groups should~~be required to~~ apply an accepted minimum standard of KYC policies and procedures on a global basis, covering foreign branches and subsidiaries

[6] The meaning of physical presence is not defined in the CDD paper. In its *Shell banks and booking offices* (July 2002) paper, the Basel Committee defines "physical presence" to be meaningful mind and management.

as well as non-bank entities. Where the minimum KYC standards of the home and host country differ, branches and subsidiaries in the host jurisdictions should be required to apply the higher standard of the two, subject to the respect of local legislation compatible with international AML/CFT standards (CDD 64, 66).

92. Banks should~~be required to~~ have a routine for testing compliance against both home and host country KYC standards (CDD 64).

VIII. Enforcement powers and sanctions

93. Compliance with customer due diligence requirements should be subject to monitoring by the supervisor, which should include the review of policies and procedures and of customer files, and the sampling of some accounts (CDD 61).

94. Supervisors should be authorised to access all documentation related to accounts, including any analysis the banks have made to detect unusual or suspicious transactions (CDD 61).

95. Supervisors should have the powers to apply appropriate sanctions in cases where banks fail to observe internal procedures and regulatory due diligence requirements (CDD 62).

96. The home supervisor should have the power to require a bank to close down an establishment in a foreign jurisdiction where there are genuine legal impediments ~~to carry~~for the home supervisor in carrying out satisfactory ~~assessments~~on site inspections which prove to be insurmountable and there are no satisfactory alternative arrangements which can be put in place (CDD 69).

IX. Co-operation between supervisors and other competent authorities

97. The host jurisdiction should permit foreign home country supervisors or auditors to carry out on-site inspections to verify compliance with home country KYC procedures and policies of local branches or subsidiaries of foreign banks. This will require a review of customer files and random sampling of accounts (CDD 68).

98. The host jurisdiction should permit access by the foreign home country supervisors or auditors to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and risk management practices. This will require a review of customer files and ~~practices~~random sampling of accounts (CDD 68).

99. There should be no impediment to sharing consolidated reporting of deposit or borrower concentration information or notification of funds under management if this information is needed by the home country supervisor (CDD 68).

100. Supervisors should have safeguards in place to ensure that information regarding individual accounts obtained through co-operative arrangements is used exclusively for lawful supervisory purposes, and can be protected by the recipient in a satisfactory manner (CDD 68).

2.2.3. Insurance sector: sector-specific criteria

~~Insurance entities[7] are expected to~~Insurers and insurance intermediaries should adopt and enforce AML/CFT policies, procedures and controls that will govern ~~the activities of their staff.~~their activities. They also need to ensure that their internal control systems are such as to ensure that policies adopted by their boards and management for preventing and deterring ML and FT are fully implemented, and that prompt follow-up action, such as reporting suspicious transactions to the FIU~~or other competent authority~~ is taken.

The IAIS Core Principles of Insurance Supervision (Insurance Core Principles or ICP). Principles 1, 2, 3, 4, 5, 10, and 16, contain criteria that are relevant for AML/CFT efforts. Most important among these principles for AML/CFT purposes are internal controls. That said, experience with ICP assessments has revealed that in many cases internal control procedures within insurance entities are not well established and supervisors have been weak in promoting their development. If management and supervisors are not able to rely on internal control systems for general operating purposes, it will be unlikely that company management and staff will have effective AML/CFT controls.

The sector-specific criteria draw extensively from the IAIS "AML Guidance Notes for insurance supervisors and insurance entities" as of January 2002. There are no additional criteria for sections I (General framework), VII (Integrity standards), VIII (Enforcement powers and sanctions), and IX (Financial Supervisors). The additional specific criteria for insurance entities are as follows:

X. Customer identification

101. The insurance entity should be required to establish to its reasonable satisfaction that every verification subject[8] relevant to the application for insurance business actually exists. All the verification subjects of joint applicants for insurance business should normally be verified. Where there are a large number of verification subjects (e.g., in the case of group life and pensions) it may be sufficient to carry out full verification requirements on a limited group only, such as the principal shareholders, the main directors of a company, etc.

102. The insurance entity should not enter into a business relationship or carry out a significant one-off transaction unless it is fully implementing the above systems. An important pre-condition of recognition of a suspicious transaction is for the insurance entity to know enough about the customer to recognise that a transaction or a series of transactions are unusual.

103. The insurance entity should be required to carry out verification in respect of the parties entering into the insurance contract. On occasion there may be underlying principals (persons on whose behalf the nominee customer is acting) and, if this is the case, the true nature of the relationship between the principals and the policyholders should be established, and appropriate inquiries performed on the former, especially if the policyholders are accustomed to act on their instruction.

~~[7] Insurance entities includes insurance companies and, where relevant, insurance intermediaries and reinsurers (as set out in the IAIS Guidance Notes).~~

[8] Verification subject refers to the person whose identity needs to be established and verified.

104. If claims, commissions, and other monies are to be paid to persons (including partnerships, companies, etc). other than the policyholder then the proposed recipients of these monies should be the subjects of verification.

XI. Ongoing monitoring of accounts and transactions

105. The insurance entity should be required to be alert to the implications of the financial flows and transaction patterns of existing policyholders, particularly where there is a significant, unexpected, and unexplained change in the behaviour of policyholders account (e.g., early surrenders). The insurance entity and the insurance supervisor should be extra vigilant to the particular risks from the practice of buying and selling second hand endowment policies, as well as the use of single premium unit-linked policies. The insurance entity should check any reinsurance or retrocession to ensure the monies are paid to bona fide re-insurance entities at rates commensurate with the risks underwritten.

XII. Record keeping

106. The supervisor should require that the insurance entity maintains records to assess: (i) initial proposal documentation including: where completed, the client financial assessment (the "fact find"), client's needs analysis, details of the payment method, illustration of benefits, and copy documentation in support of verification by the insurance entity; (ii) post-sale records associated with the maintenance of the contract, up to and including maturity of the contract; and (iii) details of the maturity processing and/or claim settlement including completed "discharge documentation."

107. The supervisor should issue guidelines and verify that if an appointed representative of the insurance entity is licensed under the insurance law in the insurance supervisor's jurisdiction then the insurance entity, as principal, can rely on the representative's assurance that the person will keep records on the insurance entity's behalf. The insurance entity may keep such records. In such a case it is important that the division of responsibilities be clearly agreed between the insurance entity and the representative. If an agency is terminated, responsibility for the integrity of such records rests with the insurance entity as product provider.

> 107.1 Rules, regulations or guidelines should specify if the appointed representative is not itself licensed, it is the direct responsibility of the insurance company or intermediary as principal to ensure that records are kept in respect of the business that such representative has introduced to it or effected on its behalf.

XIII. Suspicious transaction reporting

108. The supervisor or other competent authority should provide guidance to identify suspicious transactions. Examples may include (i) any unusual or disadvantageous early redemption of an insurance policy; (ii) any unusual employment of an intermediary in the course of some usual transaction or financial activity e.g., payment of claims or high commission to an unusual intermediary; and (iii) any unusual method of payment; transactions involving persons, companies or other entities from countries or other jurisdictions where AML/CFT measures are viewed to be inadequate.

XIV. Internal controls, Compliance and Audit

109. Guidelines should recommend that insurance and reinsurance companies foster close working relationships between underwriters and claims investigators. Reporting systems should be in place to alert senior management and/or the board of directors if AML/CFT procedures are not properly followed.

110. Consistent with Insurance Core Principle criterion 5.8, the supervisor should have the authority to require that insurance entities have an ongoing audit function of a nature and scope appropriate to the nature and scale of the business. This includes ensuring compliance with all applicable policies and procedures and reviewing whether the insurer's policies, practices, and controls remain sufficient and appropriate for its business.

2.2.4. Securities sector: sector-specific criteria

The international standards for securities regulation are set out in the "Objectives and Principles of Regulation" of the International Organization of Securities Commissions (IOSCO Core Principles) (issued in September 1998 and updated in February 2002). The IOSCO Core Principles document sets forth the objectives and principles upon which sound and effective securities regulation is based. Other IOSCO Public Documents and Resolutions also may provide further explanatory material relating to matters addressed by the IOSCO Principles. IOSCO Reports are cross-referenced to the IOSCO Principles in the February 2002 edition of the Principles. IOSCO Public Document No. 26, Report on Money Laundering, IOSCO Technical Committee, October 1992, is especially relevant. [9]

It is important to note that the IOSCO Core Principles were not created for the purpose of achieving an anti-money laundering regime. However, securities regulation complements the fight against money laundering, and the particular IOSCO Core Principles set forth below are relevant to assessing compliance with AML/CFT standards.

In assessing the securities sector for compliance with AML/CFT standards, the assessor should view ~~Sections~~sections 2.2.1 and 2.2.4 as integral components. Additionally, it is preferable that assessment of compliance with the criteria in ~~Sections~~sections 2.2.1 and 2.2.4 should be done either by or in close consultation with the assessor responsible for assessing a jurisdiction's compliance with the IOSCO Core Principles. The assessor responsible for assessing compliance with the IOSCO Core Principles will be intimately familiar with the criteria for which an IOSCO Core Principle will be deemed implemented.

There are no additional sector-specific criteria for sections I (General framework), III (Ongoing monitoring of accounts and transactions), and V (Suspicious transactions reporting). The additional specific criteria for the securities sector are as follows:

XV. Customer identification

111. A market intermediary should seek from its customers any information about their circumstances and investment objectives relevant to the services to be provided (IOSCO Core Principles, Section 12.5).[10]

IV. Record keeping

112. Policies and procedures should be established which ensure the integrity, security, availability, reliability and thoroughness of all information, including documentation and electronically stored data, relevant to the market intermediary's business operations (IOSCO Core Principles, Section 12.5).

[9] The IOSCO Principles and IOSCO Public Documents and Resolutions are available on IOSCO's website at http://www.iosco.org/iosco.html.

[10] See also the IOSCO Presidents' Committee's *Resolution on Principles for Record Keeping, Collection of Information, Enforcement Powers and Mutual Cooperation* (November 1997) and the IOSCO Multilateral MOU (May 2002).

V. Internal controls, Compliance and Audit

113. Market intermediaries should be required to comply with standards for internal organisation and operational conduct that aim to protect the interests of clients, ensure proper management of risk, and under which management of the intermediary accepts primary responsibility for these matters (IOSCO Core Principle No.23).

VI. Integrity standards

114. The licensing[11] and supervision of market intermediaries should set minimum standards for market participants (IOSCO Core Principles, section 12.3).

114.1 The licensing process should require a comprehensive assessment of the applicant and all those who are in a position to control or materially influence the applicant (IOSCO Core Principles, section 12.3).

114.2 There should be clear criteria for eligibility to operate a collective investment scheme (IOSCO Core Principles, section 11.3).

VII. Enforcement powers and sanctions

115. The supervisor should have the power to require the provision of information[12] or to carry out inspections of business operations whenever it believes it necessary to ensure compliance with relevant standards (IOSCO Core Principles, Section 8.2).

116. The supervisor or other competent authority should, therefore, be provided with comprehensive investigative and enforcement powers including, among others, regulatory and investigative powers to obtain data, information, documents, statements and records from persons involved in the relevant conduct or who may have information relevant to the inquiry; power to seek orders and/or to take other action to ensure compliance with these regulatory, administrative and investigation powers; power to impose administrative sanctions and / or to seek orders from courts or tribunals; and power to initiate or to refer matters for criminal prosecution (IOSCO Core Principles, Section 8.3).

117. Laws should provide the supervisor with adequate powers to take effective action in cases of cross-border misconduct.[13] Therefore, the supervisor should strive to ensure that it or another competent authority in its jurisdiction has the necessary authority to obtain information, including statements and documents, that may be relevant to investigating and prosecuting potential violations of laws and regulations relating to securities transactions, and that such information can be shared directly with other regulators or indirectly through

[11] In some jurisdictions, authorization or registration is used instead of licensing (see footnote 58 to the IOSCO Core Principles, section 12.3).

[12] Here the information to be provided may include records kept in the ordinary course of business, information prepared in response to a particular inquiry or as part of a regulator reporting cycle.

[13] See IOSCO Public Document No. 83, *Securities Activity on the Internet*, IOSCO Technical Committee, September 1998 (in particular, Key Recommendations 14 – 16 and text) and IOSCO Public Document No. 120, *Securities Activity on the Internet II*, IOSCO Technical Committee, June 2001.

authorities in their jurisdictions for use in investigations and prosecutions of securities violations.[14] (IOSCO Core Principles, Section 8.4)~~]~~

VIII. Co-operation between supervisors and other competent authorities

118. The supervisor should have authority to share both public and non-public information with domestic and foreign counterparts (IOSCO Core Principle No. 11).[15]

119. Cooperative mechanisms should be put into place at the international level to facilitate the detection and deterrence of cross-border misconduct and to assist in the discharge of licensing and supervisory responsibilities. Among these are memoranda of understanding (IOSCO Core Principles, Section 9.3).[16]

~~120. The form of assistance provided through international cooperation may include, among other things: assistance in obtaining public or non-public information, for example, about a license holder, listed company, shareholder, beneficial owner or a person exercising control over a license holder or company; assistance in obtaining banking, brokerage or other records; assistance in obtaining voluntary cooperation from those who may have information about the subject of an inquiry; assistance in obtaining information under compulsion - either or both the production of documents and oral testimony or statements; assistance in providing information on the regulatory processes in a jurisdiction, or in obtaining court orders, for example, urgent injunctions.[17] (IOSCO Principles, Section 9.4)~~

~~121. Information sharing and assistance arrangements, whether formal or informal, should consider~~

120. Mechanisms or arrangements for the exchange of information and provision of assistance should include: (i) assistance in obtaining public or non-public information, for example, about a license holder, listed company, shareholder, beneficial owner or a person exercising control over a license holder or company; (ii) assistance in obtaining banking, brokerage or other records; (iii) assistance in obtaining voluntary co-operation from those who may have information about the subject of an inquiry; (iv) assistance in obtaining information under compulsion—either or both the production of documents and oral testimony or statements; and (v) assistance in providing information on the regulatory process in a jurisdiction, or in obtaining court orders, for example, urgent injunctions (IOSCO Principles 9.4).

---

[14] See also IOSCO Resolution No. 39: *Resolution on Enforcement Powers* (P.C.), November 1997.

[15] See further the IOSCO Multilateral MOU (May 2002).

[16] See also IOSCO Principles, Section 11.10 and IOSCO Public Document No. 52, *Discussion Paper on International Cooperation in Relation to Cross-Border Activity of Collective Investment Schemes*, IOSCO Technical Committee, June 1996.

~~[17] IOSCO Public Document No. 41, *Report on Issues Raised for Securities and Futures Regulators by Under-Regulated and Uncooperative Jurisdictions*, IOSCO Technical Committee, October 1994.~~

2.3. Information on controls and monitoring of cash and cross border transactions

This section, based on FATF 22-23, is designed to collect information on any measures that may exist to control or monitor large cash transactions, and cross border movements of currency, monetary instruments or wire transfers. The section will not be used to assess compliance with AML/CFT criteria, but is included in the detailed assessment report to gain a broader understanding of the AML/CFT system. The questions include general financial conditions that influence the use of cash and any particular factors that have resulted in increase or decrease in the use of cash in transactions (e.g., existence of financial transaction taxes, use of credit or debit cards; limitations on size denomination of bank notes; confidence in the banking system, etc).

~~122. Has~~What has the jurisdiction done in response to the following FATF Recommendations: ~~established a system to collect from~~

"Recommendation 22

Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements."

"Recommendation 23

Countries should consider the feasibility and utility of a system where banks and other financial institutions ~~or other entities information on~~and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information." ~~certain threshold, and then process that information? Are such currency transaction reports made to the FIU for entry into a computerised database? If such a system exists, is the database adequately maintained, available to the appropriate competent authorities, and used to support law enforcement efforts? Are there adequate safeguards that ensure proper use of the information (see FATF 23)?~~

~~123. Is there a system for reporting or identifying, and recording international wire transfers above a fixed amount to the FIU or another competent authority? Do systems exist that monitor and verify the data collection system (see FATF 22, 23)?~~

~~124. Does the jurisdiction require persons to report to customs or another competent authority significant cross border movements of currency or negotiable instruments, or of high value commodities such as gold or diamonds (see FATF 22, 23)?~~

"Interpretative Note to Recommendation 22

(a) To facilitate detection and monitoring of cash transactions, without impeding in any way the freedom of capital movements, members could consider the feasibility of subjecting all cross-border transfers, above a given threshold, to verification, administrative monitoring, declaration or record keeping requirements.

~~125. If the jurisdiction~~(b) If a country discovers an unusual international shipment of currency, ~~negotiable~~monetary instruments, precious metals, ~~gems, etc. does customs or another competent authority have the power to share this information with, and co-operate with, its counterparts in the jurisdiction~~or gems, etc., it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which the shipment originated and/or to which it is destined and should co-operate with a view toward establishing the source, destination, and purpose of such shipment and toward the taking of appropriate action." ~~(see Interpretative Note to FATF 22)~~?

Annex 1 - Mapping of relationship between the AML/CFT Assessment Methodology and the FATF 40

Annex 2 - Mapping of the relationship between the AML/CFT Assessment Methodology and the FATF 8

[Annexes to be drafted ~~later~~]