**PART A:**

**Questionnaire for Technical Compliance Update**

Note: This should be provided to the APG Secretariat at least six months before the scheduled on-site visit by the assessment team.

**[Date]**

Background and Key documents

Jurisdictions should briefly note any significant changes to their AML/CFT system which have taken place since the last evaluation or since they exited the follow-up process. This includes:

* New AML/CFT laws, regulations and enforceable means;
* New competent authorities, or significant reallocation of responsibility between competent authorities.

Jurisdictions should list the principal laws and regulations in their AML/CFT system, and give a brief, high-level summary of their scope. The (translated) text of these laws should be provided to assessors. It is preferable to assign each document a unique number to ensure references are consistent. These numbers should be listed here.

Jurisdictions should list the main competent authorities responsible for AML/CFT policy and operations, and summarise their specific AML/CFT responsibilities.

*1. [Example –“Since the last evaluation, Jurisdiction X has passed the ‘Law on Suspicious Transaction Reporting (2009)’ and established an FIU. Responsibility for investigating suspicious transactions has been transferred from the Ministry of Interior to the FIU.*

*2. [Example –“The principal laws relevant to AML/CFT are:*

* *Money Laundering Act (1963) (document L1) – establishes a criminal offence of money laundering*
* *Proceeds of Crime Act (2007) (document L2) – sets a legal framework for confiscation of the proceeds of crime*
* *National Security Act (2005) (document L3) – establishes a criminal offence of terrorist financing and a legal framework for implementing targeted financial sanctions*
* *Financial Sector Act (1999) (document L4) – provides the legal basis for financial sector regulation and supervision and sets out the basic AML/CFT obligations on firms. ...*

**Risk and Context**

Jurisdictions should provide assessors with available documents about the ML/TF risks in their jurisdiction. They should list each document they provide, and briefly describe their scope. Jurisdictions should also note any important considerations about risk and context which they wish to bring to the attention of assessors. This should not duplicate information included in the documents provided. If jurisdictions wish to highlight specific contextual factors, they should provide documentation on these.

Jurisdictions should describe the size and structure of their financial and DNFBP sectors, using the tables in Annex I.

**Technical Compliance Information**

Jurisdictions should provide information on their technical compliance with each of the Criteria used in the FATF Methodology.

For each criterion, jurisdictions should, as a minimum, set out the reference (name of instrument, article or section number) that applies. Jurisdictions should refer to the *specific clauses* of their laws, enforceable means, or other mechanisms which are relevant to the criterion. *If necessary* jurisdictions should also *briefly* explain the elements of their laws, enforceable means, or other mechanisms which implement the criterion, (e.g. an outline of the procedures followed, or an explanation of the interaction between two laws). Jurisdictions should also note whether the law or enforceable means referred to has changed since the last MER or follow-up report.

The (translated) text of all relevant laws, enforceable means, and other documents should be provided separately (but as early as possible).

Jurisdictions should provide brief factual information only – there is no need for lengthy argument or interpretation. There is no need to set out each criterion in full. Information could be provided in the following form:

**Recommendation 1 – Assessing Risks and Applying a Risk Based Approach**

### 1.1: Countries[[1]](#footnote-2) should identify and assess the ML/TF risks for the country

[Example – “Jurisdiction X has conducted separate risk assessments on Money Laundering (attached as document R1) and on Terrorist Financing (edited public version attached as document R2). These risk assessments are both used as the basis for the National Strategic Plan on AML/CFT (attached as document R3) which brings together both ML and TF risks.”]

### 1.2: Countries should designate an authority or mechanism to coordinate actions to assess risks

[Example – “The Minister of Finance has overall responsibility for AML/CFT. The National Strategic Plan on AML/CFT (document R3) assigns responsibility for ML risk assessment to the National Police Authority (page 54), and for TF risk assessment to the Interior Ministry (page 55). Actions are coordinated through the National AML/CFT Coordinating Committee (terms of reference on page 52).”]

### 1.3: Countries should keep the risk assessments up-to-date

[Example – “Both ML and TF risk assessments are required to be updated on an annual basis (document R3, pages 54, 55)”]

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

[Example – “The ML risk assessment is a public document (document R1). The TF risk assessment is confidential but available to selected staff of all relevant competent authorities. A public version of the TF assessment is prepared which sets out key findings for financial institutions, and DNFBPs (document R2).”]

***Risk mitigation***

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

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

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

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

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

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

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

***Risk assessment***

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

### (a) document their risk assessments;

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

### (c) keep these assessments up to date; and

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

***Risk mitigation***

### 1.11 Financial institutions and DNFBPs should be required to:

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

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

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

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

**Recommendation 2 - National Cooperation and Coordination**

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

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

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

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

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

**Recommendation 3 - Money Laundering Offence**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Recommendation 4 - Confiscation and Provisional Measures**

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

### (a) property laundered;

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

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

### (d) property of corresponding value.

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

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

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

### (c) take steps that will prevent or void actions that prejudice the country’s ability to freeze or seize or recover property that is subject to confiscation; and

### (d) take any appropriate investigative measures.

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

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

**Recommendation 5 – Terrorist Financing Offence**

### 5.1 Countries should criminalise TF on the basis of the Terrorist Financing Convention.

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

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

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

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

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

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

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

### 5.8 It should also be an offence to:

### (a) attempt to commit the TF offence;

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

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

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

### 5.9 TF offences should be designated as ML predicate offences.

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

**Recommendation 6 – Targeted Financial Sanctions related to Terrorism and Terrorist Financing**

***Identifying and designating***

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

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

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

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

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

### (e) provide as much relevant information as possible on the proposed name ; a statement of case which contains as much detail as possible on the basis for the listing ; and (in the case of proposing names to the 1267/1989 Committee), specify whether their status as a designating state may be made known.

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

### (a) identify a competent authority or a court as having responsibility for designating persons or entities that meet the specific criteria for designation, as set forth in UNSCR 1373; as put forward either on the country’s own motion or, after examining and giving effect to, if appropriate, the request of another country.

### (b) have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolution 1373;

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

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

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

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

### (a) collect or solicit information to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation; and

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

***Freezing***

### 6.4 Countries should implement targeted financial sanctions without delay.

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

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

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

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

### (d) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

### (e) Countries should require financial institutions and DNFBPs to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

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

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

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

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

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

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

### (d) with regard to designations pursuant to UNSCR 1988, procedures to facilitate review by the 1988 Committee in accordance with any applicable guidelines or procedures adopted by the 1988 Committee, including those of the Focal Point mechanism established under UNSCR 1730;

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

### (f) publicly known procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), upon verification that the person or entity involved is not a designated person or entity; and

### (g) mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing guidance to financial institutions and other persons or entities, including DNFBPs, that may by holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

### 6.7 Countries should authorise access to frozen funds or other assets which have been determined to be necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, in accordance with the procedures set out in UNSCR 1452 and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra-)national country pursuant to UNSCR 1373.

**Recommendation 7 – Target Financial Sanctions related to Proliferation**

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

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

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

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

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

### Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

### Countries should require financial institutions and DNFBPs to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

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

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

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

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

### (b) publicly known procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), upon verification that the person or entity involved is not a designated person or entity;

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

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

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

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

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

**Recommendation 8 – Non-profit organisations (NPOs)**

***Taking a risk-based approach***

### 8.1 Countries should:

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

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

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

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

***Sustained outreach concerning terrorist financing issues***

### 8.2 Countries should:

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

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

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

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

***Targeted risk-based supervision or monitoring of NPOs***

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

### 8.4 Appropriate authorities should:

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

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

***Effective information gathering and investigation***

### 8.5 Countries should:

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

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

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

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

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

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

**Recommendation 9 – Financial Institution Secrecy Laws**

### 9.1 Financial institution secrecy laws should not inhibit the implementation of the FATF Recommendations.

**Recommendation 10 - Customer Due Diligence (CDD)**

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

***When CDD is required***

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

### (a) establishing business relations;

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

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

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

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

***Required CDD measures for all customers***

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

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

### 10.5 Financial institutions should be required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the financial institution is satisfied that it knows who the beneficial owner is.

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

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

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

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

***Specific CDD measures required for legal persons and legal arrangements***

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

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

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

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

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

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

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

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

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

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

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

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

***CDD for Beneficiaries of Life Insurance Policies***

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

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

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

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

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

***Timing of verification***

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

### (a) this occurs as soon as reasonably practicable;

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

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

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

***Existing customers***

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

***Risk-Based Approach***

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

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

***Failure to satisfactorily complete CDD***

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

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

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

***CDD and tipping-off***

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

**Recommendation 11 – Record Keeping**

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

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

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

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

**Recommendation 12 – Politically Exposed Persons (PEPs)**

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

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

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

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

### (d) conduct enhanced ongoing monitoring on that relationship.

### 12.2 In relation to domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, in addition to performing the CDD measures required under R.10, financial institutions should be required to:

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

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

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

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

**Recommendation 13 – Correspondent banking**

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

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

### (b) assess the respondent institution’s AML/CFT controls;

### (c) obtain approval from senior management before establishing new correspondent relationships; and

### (d) clearly understand the respective AML/CFT responsibilities of each institution.

### 13.2 With respect to “payable-through accounts”, financial institutions should be required to satisfy themselves that the respondent bank:

### (a) has performed CDD obligations on its customers that have direct access to the accounts of the correspondent bank; and

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

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

**Recommendation 14 – Money or Value Transfer Services (MVTS)**

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

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

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

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

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

**Recommendation 15 – New Technologies**

***New technologies***

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

### 15.2 Financial institutions should be required to:

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

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

**Virtual assets and virtual asset service providers[[2]](#footnote-3)**

*15.3 In accordance with Recommendation 1, countries should:*

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

*(b) based on their understanding of their risks, apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified; and*

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

*15.4 Countries should ensure that:*

*(a) VASPs are required to be licensed or registered[[3]](#footnote-4) at a minimum[[4]](#footnote-5):*

*(i) when the VASP is a legal person, in the jurisdiction(s) where it is created[[5]](#footnote-6); and*

*(ii) when the VASP is a natural person, in the jurisdiction where its place of business is located[[6]](#footnote-7); and*

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

*15.5 Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions to them.[[7]](#footnote-8)*

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

*(a) VASPs are subject to adequate regulation and risk-based supervision or monitoring by a competent authority[[8]](#footnote-9), including systems for ensuring their compliance with national AML/CFT requirements;*

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

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

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

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

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

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

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

*(b) R.16 – For virtual asset transfers[[9]](#footnote-10), countries should ensure that:*

*(i) originating VASPs obtain and hold required and accurate originator information and required beneficiary information[[10]](#footnote-11) on virtual asset transfers, submit[[11]](#footnote-12) the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities;*

*(ii) beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities[[12]](#footnote-13);*

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

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

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

*15.11 Countries should rapidly provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should have a legal basis for exchanging information with their foreign counterparts, regardless of the supervisors’ nature or status and differences in the nomenclature or status of VASPs.[[13]](#footnote-14)*

***Recommendation 16 – Wire Transfers***

***Ordering financial institutions***

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

### (a) Required and accurate originator information:

### (i) the name of the originator;

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

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

### (b) Required beneficiary information:

### (i) the name of the beneficiary; and

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

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

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

### (a) Required originator information:

### (i) the name of the originator; and

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

### (b) Required beneficiary information:

### (i) the name of the beneficiary; and

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

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

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

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

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

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

***Intermediary financial institutions***

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

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

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

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

***Beneficiary financial institutions***

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

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

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

***Money or value transfer service operators***

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

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

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

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

***Implementation of Targeted Financial Sanctions***

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

**Recommendation 17 – Reliance on Third Parties**

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

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

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

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

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

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

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

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

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

**Recommendation 18 – Internal Controls and Foreign Branches and Subsidiaries**

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

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

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

### (c) an ongoing employee training programme; and

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

### 18.2 Financial groups should be required to implement group-wide programmes against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group. These should include the measures set out in criterion 18.1 and also:

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

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

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

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

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

**Recommendation 19 – Higher Risk Countries**

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

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

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

**Recommendation 20 – Reporting of Suspicious Transactions**

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

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

**Recommendation 21 – Tipping-off and Confidentiality**

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

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

**Recommendation 22 – Designated Non-Financial Businesses and Professions (DNFBPs): Customer Due Diligence**

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

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

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

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

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

### - buying and selling of real estate;

### - managing of client money, securities or other assets;

### - management of bank, savings or securities accounts;

### - organisation of contributions for the creation, operation or management of companies;

### - creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

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

*- acting as a formation agent of legal persons;*

*- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;*

*- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;*

*- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;*

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

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

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

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

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

**Recommendation 23 – DNFBPs: Other Measures**

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

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

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

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

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

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

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

**Recommendation 24 – Transparency and Beneficial Ownership of Legal Persons**

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

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

***Basic Information***

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

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

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

***Beneficial Ownership Information***

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

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

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

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

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

### 24.8 Countries should ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner, by:

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

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

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

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

***Other Requirements***

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

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

### (a) prohibiting bearer shares and share warrants; or

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

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

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

### (e) using other mechanisms identified by the country.

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

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

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

### (c) using other mechanisms identified by the country.

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

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

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

### (b) exchanging information on shareholders; and

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

### 24.15 Countries should monitor the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.

**Recommendation 25 – Transparency and Beneficial Ownership of Legal Arrangements**

### 25.1 Countries should require:

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

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

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

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

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

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

### 25.5 Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to information held by trustees, and other parties (in particular information held by financial institutions and DNFBPs), on the beneficial ownership and control of the trust, including: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction.

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

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

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

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

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

### 25.8 Countries should ensure that there are proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to grant to competent authorities timely access to information regarding the trust referred to in criterion 25.1.

**Recommendation 26 – Regulation and Supervision of Financial Institutions**

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

***Market Entry***

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

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

***Risk-based approach to supervision and monitoring***

### 26.4 Financial institutions should be subject to:

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

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

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

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

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

### (c) the characteristics of the financial institutions or groups, in particular the diversity and number of financial institutions and the degree of discretion allowed to them under the RBA.

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

**Recommendation 27 – Powers of Supervisors**

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

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

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

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

**Recommendation 28 – Regulation and Supervision of DNFBPs**

***Casinos***

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

### (a) Countries should require casinos to be licensed.

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

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

***DNFBPs other than casinos***

### 28.2 There should be a designated competent authority or self-regulatory body (SRB) responsible for monitoring and ensuring compliance of DNFBPs with AML/CFT requirements.

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

### 28.4 The designated competent authority or SRB should:

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

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

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

***All DNFBPs***

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

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

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

**Recommendation 29 – Financial Intelligence Unit (FIU)**

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

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

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

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

### 29.3 The FIU should:

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

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

### 29.4 The FIU should conduct:

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

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

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

### 29.6 The FIU should protect information by:

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

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

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

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

### (a) having the authority and capacity to carry out its functions freely, including the autonomous

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

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

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

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

**Recommendation 30 – Responsibilities of Law Enforcement and Investigative Authorities**

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

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

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

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

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

**Recommendation 31 – Powers of Law Enforcement and Investigative Authorities**

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

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

### (b) the search of persons and premises;

### (c) taking witness statements; and

### (d) seizing and obtaining evidence.

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

### (a) undercover operations;

### (b) intercepting communications;

### (c) accessing computer systems; and

### (d) controlled delivery.

### 31.3 Countries should have mechanisms in place:

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

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

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

**Recommendation 32 – Cash Couriers**

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

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

### (a) A written declaration system for all travellers;

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

### (c) An oral declaration system for all travellers.

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

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

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

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

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

### 32.8 Competent authorities should be able to stop or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/TF may be found in cases:

### (a) where there is a suspicion of ML/TF or predicate offences; or

### (b) where there is a false declaration or false disclosure.

### 32.9 Countries should ensure that the declaration/disclosure system allows for international co-operation and assistance, in accordance with Recommendations 36 to 40. To facilitate such co-operation, information shall be retained when:

### (a) a declaration or disclosure which exceeds the prescribed threshold is made; or

### (b) there is a false declaration or false disclosure; or

### (c) there is a suspicion of ML/TF.

### 32.10 Countries should ensure that strict safeguards exist to ensure proper use of information collected through the declaration/disclosure systems, without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

### 32.11 Persons who are carrying out a physical cross-border transportation of currency or BNIs that are related to ML/TF or predicate offences should be subject to: (a) proportionate and dissuasive sanctions, whether criminal, civil or administrative; and (b) measures consistent with Recommendation 4 which would enable the confiscation of such currency or BNIs.

**Recommendation 33 – Statistics**

### 33.1 Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include keeping statistics on:

### (a) Suspicious transaction reports, received and disseminated;

### (b) ML/TF investigations, prosecutions and convictions;

### (c) Property frozen; seized and confiscated; and

### (d) Mutual legal assistance or other international requests for co-operation made and received.

**Recommendation 34 – Guidance and Feedback**

### 34.1 Competent authorities, supervisors, and SRBs should establish guidelines and provide feedback, which will assist financial institutions and DNFBPs in applying national AML/CFT measures, and in particular, in detecting and reporting suspicious transactions.

**Recommendation 35 – Sanctions**

### 35.1 Countries should ensure that there is a range of proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons that fail to comply with the AML/CFT requirements of Recommendations 6, and 8 to 23.

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

**Recommendation 36 – International Instruments**

### 36.1 Countries should become a party to the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption (the Merida Convention) and the Terrorist Financing Convention.

### 36.2 Countries should fully implement the Vienna Convention, the Palermo Convention, the Merida Convention and the Terrorist Financing Convention.

**Recommendation 37 – Mutual Legal Assistance**

### 37.1 Countries should have a legal basis that allows them to rapidly provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions and related proceedings.

### 37.2 Countries should use a central authority, or another established official mechanism, for the transmission and execution of requests. There should be clear processes for the timely prioritisation and execution of mutual legal assistance requests. To monitor progress on requests, a case management system should be maintained.

### 37.3 Mutual legal assistance should not be prohibited or made subject to unreasonable or unduly restrictive conditions.

### 37.4 Countries should not refuse a request for mutual legal assistance:

### (a) on the sole ground that the offence is also considered to involve fiscal matters; or

### (b) on the grounds of secrecy or confidentiality requirements on financial institutions or DNFBPs, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies.

### 37.5 Countries should maintain the confidentiality of mutual legal assistance requests that they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry.

### 37.6 Where mutual legal assistance requests do not involve coercive actions, countries should not make dual criminality a condition for rendering assistance.

### 37.7 Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

### 37.8 Powers and investigative techniques that are required under R.31 or otherwise available to domestic competent authorities should also be available for use in response to requests for mutual legal assistance, and, if consistent with the domestic framework, in response to a direct request from foreign judicial or law enforcement authorities to domestic counterparts. These should include:

### (a) all of the specific powers required under R.31 relating to the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons, and the taking of witness statements; and

### (b) a broad range of other powers and investigative techniques.

**Recommendation 38 – Mutual Legal Assistance: Freezing and Confiscation**

### 38.1 Countries should have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize, or confiscate:

### (a) laundered property from,

### (b) proceeds from,

### (c) instrumentalities used in, or

### (d) instrumentalities intended for use in, money laundering, predicate offences, or terrorist financing; or

### (e) property of corresponding value.

### 38.2 Countries should have the authority to provide assistance to requests for cooperation made on the basis of non-conviction based confiscation proceedings and related provisional measures, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown, unless this is inconsistent with fundamental principles of domestic law.

### 38.3 Countries should have: (a) arrangements for co-ordinating seizure and confiscation actions with other countries; and (b) mechanisms for managing, and when necessary disposing of, property frozen, seized or confiscated.

### 38.4 Countries should be able to share confiscated property with other countries, in particular when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

**Recommendation 39 - Extradition**

### 39.1 Countries should be able to execute extradition requests in relation to ML/TF without undue delay. In particular, countries should:

### (a) ensure ML and TF are extraditable offences;

### (b) ensure that they have a case management system, and clear processes for the timely execution of extradition requests including prioritisation where appropriate; and

### (c) not place unreasonable or unduly restrictive conditions on the execution of requests.

### 39.2 Countries should either:

### (a) extradite their own nationals; or

### (b) where they do not do so solely on the grounds of nationality, should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request.

### 39.3 Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

### 39.4 Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms in place.

**Recommendation 40 – Other Forms of International Cooperation**

***General Principles***

### 40.1 Countries should ensure that their competent authorities can rapidly provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Such exchanges of information should be possible both spontaneously and upon request.

### 40.2 Competent authorities should:

### (a) have a lawful basis for providing cooperation;

### (b) be authorised to use the most efficient means to cooperate;

### (c) have clear and secure gateways, mechanisms or channels that will facilitate and allow for the transmission and execution of requests;

### (d) have clear processes for the prioritisation and timely execution of requests; and

### (e) have clear processes for safeguarding the information received.

### 40.3 Where competent authorities need bilateral or multilateral agreements or arrangements to cooperate, these should be negotiated and signed in a timely way, and with the widest range of foreign counterparts.

### 40.4 Upon request, requesting competent authorities should provide feedback in a timely manner to competent authorities from which they have received assistance, on the use and usefulness of the information obtained.

### 40.5 Countries should not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of exchange of information or assistance. In particular, competent authorities should not refuse a request for assistance on the grounds that:

### (a) the request is also considered to involve fiscal matters; and/or

### (b) laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies); and/or

### (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or

### (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

### 40.6 Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only for the purpose for, and by the authorities, for which the information was sought or provided, unless prior authorisation has been given by the requested competent authority.

### 40.7 Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, consistent with both parties’ obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Competent authorities should be able to refuse to provide information if the requesting competent authority cannot protect the information effectively.

### 40.8 Competent authorities should be able to conduct inquiries on behalf of foreign counterparts, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

***Exchange of Information between FIUs***

### 40.9 FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing.

### 40.10 FIUs should provide feedback to their foreign counterparts, upon request and whenever possible, on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

### 40.11 FIUs should have the power to exchange:

### (a) all information required to be accessible or obtainable directly or indirectly by the FIU, in particular under Recommendation 29; and

### (b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.

***Exchange of information between financial supervisors***

### 40.12 Financial supervisors should have a legal basis for providing cooperation with their foreign counterparts (regardless of their respective nature or status), consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

### 40.13 Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, in a manner proportionate to their respective needs.

### 40.14 Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other supervisors that have a shared responsibility for financial institutions operating in the same group:

### (a) regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors;

### (b) prudential information, in particular for Core Principles supervisors, such as information on the financial institution’s business activities, beneficial ownership, management, and fit and properness; and

### (c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

### 40.15 Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

### 40.16 Financial supervisors should ensure that they have the prior authorisation of the requested financial supervisor for any dissemination of information exchanged, or use of that information for supervisory and non-supervisory purposes, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation.

***Exchange of information between law enforcement authorities***

### 40.17 Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.

### 40.18 Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement co-operation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority.

### 40.19 Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangements to enable such joint investigations.

***Exchange of information between non-counterparts***

### 40.20 Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Countries should ensure that the competent authority that requests information indirectly always makes it clear for what purpose and on whose behalf the request is made.

### Annex 1 to the questionnaire for technical compliance update: size and structure of the financial and DNFBP sectors

**AML/CFT Preventive Measures for Financial Institutions and DNFBPs (R.10 to R.23)**

| **Type of Entity\*** | **No. Licensed / Regulated / Registered** | **AML/CFT Laws\*\* / Enforceable Means for Preventive Measures** | **Date in Force or Last Updated**  **(*where applicable*)** | **Other additional Information (*e.g.* highlights of substantive changes etc.)\*\*\*** |
| --- | --- | --- | --- | --- |
| **Banks** |  |  |  |  |
| **Life Insurers** |  |  |  |  |
| **Securities** |  |  |  |  |
| **MVTS** |  |  |  |  |
| **Casinos** |  |  |  |  |
| **Lawyers** |  |  |  |  |
| **Notaries** |  |  |  |  |
| **Accountants** |  |  |  |  |
| **Precious Metals & Stones Dealers** |  |  |  |  |
| **Trust and Company Service Providers** |  |  |  |  |
| **Others** |  |  |  |  |

\*Additional rows may be added for other type of financial institutions and DNFBPs. Jurisdictions may also choose to have more granular and specific classification of the types of financial institutions and DNFBPs.

\*\* Jurisdictions should indicate the specific provisions in the AML/CFT laws that set out the CDD, record keeping and STR reporting obligations.

\*\*\*Where there have been changes since its last update or where relevant, jurisdictions should also set out the specific provisions in the AML/CFT laws or enforceable means and key highlights of the obligations for other preventive measures (*e.g.* PEPs, wire transfers, internal controls and foreign branches and subsidiaries etc.).

**Legal Persons and Arrangements (R.8, R.24 and R.25)**

| **Type of Legal Persons / Arrangements\*** | **No. Registered (where available)** | **Applicable Laws / Regulations / Requirements** | **Date in Force or Last Updated**  **(*where applicable*)** | **Other additional Information (*e.g.* highlights of substantive changes etc.)\*\*** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

\*Additional rows may be added for other type of legal persons or arrangements. Jurisdictions may also choose to have more granular and specific classification of the types of legal persons or arrangements. \*\* Jurisdictions should indicate the specific provisions in the applicable laws / regulations / requirements and key highlights that set out the obligations to maintain the requisite information in R.24 (*e.g.* basic and beneficial ownership) and R.25 (*e.g.* settlors, trustees, protectors (if any), the (class of) beneficiaries, and any other natural person exercising control) respectively.

## **Appendix 4 (b) – Template on Effectiveness Response**

**PART B:**

**RESPONSE TO THE CORE ISSUES ON THE 11 IMMEDIATE OUTCOMES ON EFFECTIVENESS**

Please note the following:

1. The response on effectiveness for the 11 Immediate Outcomes should be provided to the APG Secretariat at least four months before the scheduled on-site visit by the assessment team.
2. There is no formal questionnaire template for the response on effectiveness. The format provided is essentially a copy of the core issues for each of the 11 Immediate Outcomes on effectiveness as specified in the FATF Methodology. Use of the format is voluntary.
3. When providing your response, please consult the full FATF Methodology as it lists a lot of specific information which might be relevant to each of the 11 Immediate Outcomes.

**[Date]**

**BACKGROUND**

Jurisdictions should provide information on effectiveness based on the 11 Immediate Outcomes identified in the effectiveness assessment methodology no less than 4 months before the on-site. They should set out fully how each of the core issues is being addressed as set out in each Immediate Outcome. It is important for jurisdictions to provide a full and accurate description (including examples of information, data and other factors) that would help to demonstrate the effectiveness of the AML/CFT regime.

The single most helpful thing you can do in this area is to provide a narrative explanation of the evidence.

The assessors can work with raw information, but it takes a long time to understand it properly – assessors have to work out:

What it tells, and which part of the effectiveness framework it relates to?

How important it is – is it critical or just an additional supporting piece of information?

How does it relate to other information – does it support or explain some other item?

A short narrative explanation can set out your understanding of those high-level questions i.e. your understanding of how your jurisdiction meets a particular outcome or a specific core issue, which says which factors and which evidence are most important to your view, and how you would interpret them. This is not a long text, with a specific format or template – it would only be useful if it clearly and simply sets out your understanding of the issue, as a very brief starting point to help the assessors assimilate the information you provide.

One way to think of this is that for each outcome or for each core issue, you will provide us with a dossier of several different documents which show your effectiveness. A narrative would be the covering note or the introduction to the dossier – explaining what is included and why.

**Providing statistics**

Statistics that are provided should:

1. **Have a context** – assessors need to know what they show, where they come from, and whether there are specific factors that explain any trends or specific data points.

2. **Be coherent** – data should be clear about sources of information, the units used, time periods etc. Data derived from different sources should be similar.

3. **Relevant**: The statistical product should meet the needs of assessors and relate to the assessment of effectiveness.

4**. Accurate**: In AML/CFT, countries should be conscious that many data are proxies or estimates and may suffer from the following non-sampling errors: coverage error, non-response error, measurement error, processing error, and model assumption error.

5. **Comparable**: AML/CFT data to be useful needs to be comparable over time; spatial domains (e.g. sub-national, national, international); domain or sub-population (e.g. sectors, agency outputs or outcomes).

6. **Timely**: Statistics should be timely relevant to the on-site visit.

7. **Accessible and clear**: Statistics need to be accessible by assessors. This means that the format(s) in which the data are available, and the supporting information, should ensure that the information isclear and assessors can understand it. Illustrations and accompanying advice should be provided to assist.

The focus for assessors will be the analysis showing if the outcome is being achieved rather than raw data. Assessors will be interpreting the available data critically, in the context of the jurisdiction’s circumstances.

There are specific problems that should be avoided:

Prosecution and conviction data often mixes predicate offense & ML/TF

Reporting may not distinguish STRs & other types of reports (e.g., CTRs)

Some data may be based on subjective interpretations

Double counting and the use of inconsistent time periods and definitions (particularly if aggregating data from provincial or state level, or from different agencies).

Data on its own is meaningless. Jurisdictions should provide context, not just raw data. For example, if a significant change in statistics, explain why this may be the case.

**Providing documents**

Data and statistics are important, but this is not just an exercise in data analysis – statistics are notoriously hard to analyse in the AML/CFT world. So we need other information in order to complete the picture:

1. Information on the risks, the context, and the relevance of different activities and sectors is vital to understanding and analysing any hard numerical data the assessors have.

2. Case studies or examples can help understand how – and how well – the system works in practice. There is room for success stories, even if they are not representative of all day-to-day activity.

3. Publicly available documents such as relevant laws, regulations, annual reports, guidance documents etc are very important for assessors.

4. Internal documents can also be very important – and they could include internal policies or procedures, international cooperation agreements, memoranda of understanding, etc.

There are two fundamental points to remember about documentation.

- In the FATF Methodology, it is the assessed jurisdiction’s responsibility to demonstrate its effectiveness.

- The second is that we recognise that a lot of information in this area is sensitive – sometimes very sensitive, either for national security or for commercial reasons. We are very willing to have redacted copies of documents, or to look at documents which we are not allowed to take copies of or refer to.

**Immediate Outcome 1**: Money laundering and terrorist financing risks are understood and, where appropriate, actions co-ordinated domestically to combat money laundering and the financing of terrorism and proliferation

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

* 1. How well does the country understand its ML/TF risks?
  2. How well are the identified ML/TF risks addressed by national AML/CFT policies and activities?
  3. To what extent are the results of the assessment(s) of risks properly used to justify exemptions and support the application of enhanced measures for higher risk scenarios, or simplified measures for lower risk scenarios?
  4. To what extent are the objectives and activities of the competent authorities and SRBs consistent with the evolving national AML/CFT policies and with the ML/TF risks identified?
  5. To what extent do the competent authorities and SRBs co-operate and co-ordinate the development and implementation of policies and activities to combat ML/TF and, where appropriate, the financing of proliferation of weapons of mass destruction?
  6. To what extent does the country ensure that respective financial institutions, DNFBPs and other sectors affected by the application of the FATF Standards are aware of the relevant results of the national ML/TF risks?

**Immediate Outcome 2**: International co-operation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.

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

* 1. To what extent has the country provided constructive and timely mutual legal assistance and extradition across the range of international co-operation requests? What is the quality of such assistance provided?
  2. To what extent has the country sought legal assistance for international co-operation in an appropriate and timely manner to pursue domestic ML, associated predicate offences and TF cases which have transnational elements?
  3. To what extent do the different competent authorities seek other forms of international cooperation to exchange financial intelligence and supervisory, law enforcement or other information in an appropriate and timely manner with their foreign counterparts for AML/CFT purposes?
  4. To what extent do the different competent authorities provide (including spontaneously) other forms of international co-operation to exchange financial intelligence and supervisory, law enforcement or other information in a constructive and timely manner with their foreign counterparts for AML/CFT purposes?
  5. How well are the competent authorities providing and responding to foreign requests for co-operation in identifying and exchanging basic and beneficial ownership information of legal persons and arrangements?

**Immediate Outcome 3:** Supervisors appropriately supervise, monitor and regulate financial

Institutions,DNFBPs and VASPs for compliance with AML/CFT requirements commensurate with their risks.

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

* 1. How well does licensing, registration or other controls implemented by supervisors or other authorities prevent criminals and their associates from holding, or being the beneficial owner of a significant or controlling interest or holding a management function in financial institutions, DNFBPs or VASPs? How well are breaches of such licensing or registration requirements detected?
  2. How well do the supervisors identify and maintain an understanding of the ML/TF risks in the financial and other sectors as a whole, between different sectors and types of institution, and of individual institutions?
  3. With a view to mitigating the risks, how well do supervisors, on a risk-sensitive basis, supervise or monitor the extent to which financial institutions, DNFBPs and VASPs are complying with their AML/CFT requirements?
  4. To what extent are remedial actions and/or effective, proportionate and dissuasive sanctions applied in practice?
  5. To what extent are supervisors able to demonstrate that their actions have an effect on compliance by financial institutions, DNFBPs and VASPs?
  6. How well do the supervisors promote a clear understanding by financial institutions, DNFBPs and VASPs of their AML/CFT obligations and ML/TF risks?

**Immediate Outcome 4:** Financial institutions,DNFBPs and VASPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.

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

* 1. How well do financial institutions, DNFBPs and VASPs understand their ML/TF risks and AML/CFT obligations?
  2. How well do financial institutions, DNFBPs and VASPs apply mitigating measures commensurate with their risks?
  3. How well do financial institutions, DNFBPs and VASPs apply the CDD and record-keeping measures (including beneficial ownership information and ongoing monitoring)? To what extent is business refused when CDD is incomplete?
  4. How well do financial institutions,DNFBPs and VASPs apply the enhanced or specific measures for: (a) PEPs, (b) correspondent banking, (c) new technologies, (d) wire transfers rules, (e) targeted financial sanctions relating to TF, and (f) higher-risk countries identified by the FATF?
  5. To what extent do financial institutions,DNFBPs and VASPs meet their reporting obligations on the suspected proceeds of crime and funds in support of terrorism? What are the practical measures to prevent tipping-off?
  6. How well do financial institutions,DNFBPs and VASPs apply internal controls and procedures (including at financial group level) to ensure compliance with AML/CFT requirements? To what extent are there legal or regulatory requirements (e.g., financial secrecy) impeding its implementation?

**Immediate Outcome 5:** Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments.

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

* 1. To what extent is the information on the creation and types of legal persons and arrangements in the country available publicly?
  2. How well do the relevant competent authorities identify, assess and understand the vulnerabilities and the extent to which legal persons created in the country can be, or are being misused for ML/TF?
  3. How well has the country implemented measures to prevent the misuse of legal persons and arrangements for ML/TF purposes?
  4. To what extent can relevant competent authorities obtain adequate, accurate and current basic and beneficial ownership information on all types of legal persons created in the country, in a timely manner?
  5. To what extent can relevant competent authorities obtain adequate, accurate and current beneficial ownership information on legal arrangements, in a timely manner?
  6. To what extent are effective, proportionate and dissuasive sanctions applied against persons who do not comply with the information requirements?

**Immediate Outcome 6:** Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.

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

* 1. To what extent are financial intelligence and other relevant information accessed and used in investigations to develop evidence and trace criminal proceeds related to ML, associated predicate offences and TF?
  2. To what extent are the competent authorities receiving or requesting reports (e.g., STRs, reports on currency and bearer negotiable instruments) that contain relevant and accurate information that assists them to perform their duties?
  3. To what extent is FIU analysis and dissemination supporting the operational needs of competent authorities?
  4. To what extent do the FIU and other competent authorities co-operate and exchange information and financial intelligence? How securely do the FIU and competent authorities protect the confidentiality of the information they exchange or use?

**Immediate Outcome 7:** Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.

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

* 1. How well, and in what circumstances are potential cases of ML identified and investigated (including through parallel financial investigations)?
  2. To what extent are the types of ML activity being investigated and prosecuted consistent with the country’s threats and risk profile and national AML/CFT policies?
  3. To what extent are different types of ML cases prosecuted (e.g., foreign predicate offence, third-party laundering, stand-alone offence etc.) and offenders convicted?
  4. To what extent are the sanctions applied against natural or legal persons convicted of ML offences effective, proportionate and dissuasive?
  5. To what extent do countries apply other criminal justice measures in cases where a ML investigation has been pursued but where it is not possible, for justifiable reasons, to secure a ML conviction? Such alternative measures should not diminish the importance of, or be a substitute for, prosecutions and convictions for ML offences.

**Immediate Outcome 8:** Proceeds and instrumentalities of crime are confiscated.

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

* 1. To what extent is confiscation of criminal proceeds, instrumentalities and property of equivalent value pursued as a policy objective?
  2. How well are the competent authorities confiscating (including repatriation, sharing and restitution) the proceeds and instrumentalities of crime, and property of an equivalent value, involving domestic and foreign predicate offences and proceeds which have been moved to other countries?
  3. To what extent is confiscation regarding falsely / not declared or disclosed cross-border movements of currency and bearer negotiable instruments being addressed and applied as an effective, proportionate and dissuasive sanction by border/custom or other relevant authorities?
  4. How well do the confiscation results reflect the assessments(s) of ML/TF risks and national AML/CFT policies and priorities?

**Immediate Outcome 9:** Terrorist financing offences and activities are investigated andpersons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.

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

* 1. To what extent are the different types of TF activity (e.g., collection, movement and use of funds or other assets) prosecuted and offenders convicted? Is this consistent with the country’s TF risk profile?
  2. How well are cases of TF identified, and investigated? To what extent do the investigations identify the specific role played by the terrorist financier?
  3. To what extent is the investigation of TF integrated with, and used to support, national counter-terrorism strategies and investigations (e.g., identification and designation of terrorists, terrorist organisations and terrorist support networks)?
  4. To what extent are the sanctions or measures applied against natural and legal persons convicted of TF offences effective, proportionate and dissuasive?
  5. To what extent is the objective of the outcome achieved by employing other criminal justice, regulatory or other measures to disrupt TF activities where it is not practicable to secure a TF conviction?

**Immediate Outcome 10:** Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.

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

* 1. How well is the country implementing targeted financial sanctions pursuant to (i) UNSCR1267 and its successor resolutions, and (ii) UNSCR1373 (at the supra-national or national level, whether on the country’s own motion or after examination, to give effect to the request of another country)?
  2. To what extent, without disrupting or discouraging legitimate NPO activities, has the country applied focused and proportionate measures to such NPOs which the country has identified as being vulnerable to terrorist financing abuse, in line with the risk-based approach?
  3. To what extent are terrorists, terrorist organisations and terrorist financiers deprived (whether through criminal, civil or administrative processes) of assets and instrumentalities related to TF activities?
  4. To what extent are the above measures consistent with the overall TF risk profile?

**Immediate Outcome 11:** Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

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

* 1. How well is the country implementing, without delay, targeted financial sanctions concerning the UNSCRs relating to the combating of financing of proliferation?
  2. To what extent are the funds or other assets of designated persons and entities (and those acting on their behalf or at their direction) identified and such persons and entities prevented from operating or executing financial transactions related to proliferation?
  3. To what extent do financial institutions,DNFBPs and VASPs comply with, and understand their obligations regarding targeted financial sanctions relating to financing of proliferation?
  4. How well are relevant competent authorities monitoring and ensuring compliance by financial institutions,DNFBPs and VASPs with their obligations regarding targeted financial sanctions relating to financing of proliferation?

1. Where appropriate, ML/TF risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied. [↑](#footnote-ref-2)
2. Note to assessors: Countries that have decided to prohibit virtual assets should only be assessed under criteria 15.1, 15.2, 15.3(a) and 15.3(b), 15.5 and 15.11, as the remaining criteria are not applicable in such cases. [↑](#footnote-ref-3)
3. A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations. [↑](#footnote-ref-4)
4. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. [↑](#footnote-ref-5)
5. References to creating a legal person include incorporation of companies or any other mechanism that is used. To clarify, the requirement in criterion 15.4(a)(i) is that a country must ensure that a VASP created within the country is licenced or registered, but not that any VASP licenced or registered in the country is also registered in any third country where it was created. [↑](#footnote-ref-6)
6. To clarify, criterion 15.4(a)(ii) requires that a country ensure that a VASP that is a natural person located in their country is licensed or registered in their country; not that any VASP that is a natural person with a place of business located in the country is registered in any third country where it also has a place of business. [↑](#footnote-ref-7)
7. Note to assessors: Criterion 15.5 applies to all countries, regardless of whether they have chosen to license, register or prohibit virtual assets or VASPs. [↑](#footnote-ref-8)
8. In this context, a “competent authority” cannot include a SRB. [↑](#footnote-ref-9)
9. For the purposes of applying R.16 to VASPs, all virtual asset transfers should be treated as cross-border transfers. [↑](#footnote-ref-10)
10. As defined in INR.16, paragraph 6, or the equivalent information in a virtual asset context. [↑](#footnote-ref-11)
11. The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to virtual asset transfers. [↑](#footnote-ref-12)
12. *Appropriate authorities* means *appropriate competent authorities*, as referred to in paragraph 10 of INR.16. [↑](#footnote-ref-13)
13. Countries that have prohibited VASPs should fulfil this requirement by having in place a legal basis for permitting their relevant competent authorities (e.g. law enforcement agencies) to exchange information on issues related to VAs and VASPs with non-counterparts, as set out in paragraph 17 of INR.40. [↑](#footnote-ref-14)