APG THIRD ROUND MUTUAL EVALUATION PROCEDURES 2014

FOR AML/CFT

JULY 2014

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for *Combating the financing of terrorism*)
APG	Asia/Pacific Group on Money Laundering
CDD	Customer due diligence
DNFBP	Designated Non-Financial Business or Profession
ES	Executive Summary
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSAP	Financial Sector Assessment Programme
FSRB	FATF-Style Regional Body
GIFCS	Group of International Finance Centre Supervisors
IO	Immediate Outcome
IFI	International Financial Institution (IMF and World Bank)
MER	Mutual Evaluation Report
MEWG	Mutual Evaluation Working Group
ML	Money laundering
NC	Non-compliant
PC	Partially compliant
STR	Suspicious transaction report
SRB	Self-Regulatory Body
TC	Technical compliance
TF	Terrorist financing

APG THIRD ROUND MUTUAL EVALUATION PROCEDURES FOR AML/CFT 2014

Introduction

1. The APG is conducting a third round of mutual evaluations of its members based on the FATF Recommendations (2012), and the Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems ("the 2013 Assessment Methodology"), as amended from time to time. This document sets out the procedures that are the basis for that third round of mutual evaluations.

Background

2. At the APG's 2012 Annual Meeting, APG members:

    - Adopted the 2012 FATF 40 Recommendations, as part of the adoption of the APG Terms of Reference 2012;
    - Agreed on the completion of the APG's second round of mutual evaluations under the Revised Procedures for APG Mutual Evaluations 2012; and
    - Adopted the APG's Third Round Mutual Evaluation Schedule, noting that it is likely to be subject to change.

3. At the FATF's October 2012 Plenary, the FATF :

    - Adopted the High Level Principles and Objectives for FATF and FATF-style regional bodies (FSRBs), which include a set of core elements on mutual evaluations which should apply to all AML/CFT assessment bodies.

4. At the APG's 2013 Annual Meeting, APG members:

    - Agreed that the APG would use the 2013 Assessment Methodology for all APG mutual evaluations occurring in the APG's third round of evaluations;
    - Adopted key mutual evaluation principles, and approaches for developing the APG third round mutual evaluation procedures; and
    - Agreed to phase out the Second Round Mutual Evaluation Follow-Up Procedures by July 2015.

5. At the FATF's February 2014 Plenary, the FATF:

    - Adopted the Universal Procedures for AML/CFT Assessments (Including on Quality and Consistency) that should form the basis for the evaluations conducted by all AML/CFT assessment bodies.

6. At the APG's 2014 Annual Meeting, APG members:

    - Adopted the APG Third Round Mutual Evaluation Procedures for AML/CFT 2014; and
    - Noted that the Procedures are consistent with the Universal Procedures for AML/CFT Assessments (Including on Quality and Consistency).

I. Scope, principles and objectives for the third round

7. Using the 2013 Assessment Methodology, APG members (and observers, where agreed by members) may be assessed in one of four ways:

   i. by an APG mutual evaluation;

   ii. by a joint FATF/APG evaluation, or by the International Monetary Fund or World Bank (the IFIs), for members of the APG who are also members of the FATF. Where the member is also a member of another FSRB, the evaluation may be conducted as an FATF/APG/FSRB evaluation;

   iii. by an IFI assessment; or

   iv. by a joint APG/FATF-style regional body (FSRB) or Group of International Finance Centre Supervisors (GIFCS) evaluation, or the IFIs, for members of the APG who are also members of another FSRB or the GIFCS, but not members of the FATF.

8. In each case, the APG will need to consider and adopt the mutual evaluation report (MER)/detailed assessment report (DAR) of the APG member, irrespective of which body undertook the evaluation.

9. As set out in the 2013 Assessment Methodology, the scope of evaluations will involve two inter-related components: technical compliance and effectiveness. The technical compliance component will assess whether the necessary laws, regulations or other required measures are in force and effect, and whether the supporting AML/CFT institutional framework is in place. The effectiveness component will assess whether the AML/CFT systems are working, and the extent to which the member is achieving the defined set of outcomes.

10. There are a number of general principles and objectives that govern procedures for APG mutual evaluations, as well as AML/CFT assessments conducted by the FATF, other FSRBs, IMF or World Bank. The procedures should:

    a) Produce objective and accurate reports of a high standard in a timely way.
    b) Ensure that there is a level playing field, whereby mutual evaluation reports (MERs), including the executive summaries, are consistent, especially with respect to the findings, the recommendations and ratings.
    c) Ensure that there is transparency and equality of treatment, in terms of the assessment process, for all members assessed.
    d) Seek to ensure that the evaluations and assessment exercises conducted by all relevant organisations and bodies (APG, FATF, IMF, World Bank, other FSRBs, GIFCS) are equivalent, and of a high standard.
    e) (i) Be clear and transparent; (ii) encourage the implementation of higher standards, (iii) identify and promote good and effective practices, and (iv) alert governments and the private sector to areas that need strengthening.
    f) Be sufficiently streamlined and efficient to ensure that there are no unnecessary delays or duplication in the process and that resources are used effectively.

II. Changes in the FATF Standards

11. As a dynamic process, ongoing work within the FATF could lead to further changes to the FATF Recommendations, the Interpretive Notes or the 2013 Assessment Methodology. All members should be evaluated on the basis of the FATF Recommendations and Interpretative Notes, and the 2013 Assessment Methodology, as they exist at the date of the member's on-site visit. The report should state clearly if an assessment has been made against recently amended Standards. To ensure equality

of treatment, and to protect the international financial system, compliance with the relevant elements of the changes could be assessed as part of the follow-up process (see section IX below), if they have not been assessed or as part of the mutual evaluation.

III. Schedule for the third round

12. The schedule of mutual evaluations for the third round, and the number of evaluations to be prepared each year, is primarily governed by the number of MERs that can be discussed at each APG Annual Meeting, and by the need to complete the entire round in a reasonable timeframe and by the end of the APG's current mandate (2020). On this basis, normally seven MERs would need to be discussed per Annual Meeting during the third round. However, noting changes made by the FATF in June 2014 to its 4th round schedule for resource and other concerns, which also arise in the APG, members agreed at the 2014 Annual Meeting to extend the 3rd round schedule by three years to conclude in 2023, and to reduce the average number of evaluations from seven (7) per year to approximately five (5) per year.

13. A schedule of mutual evaluations showing the proposed year and indicative date of the on-site visit, the dates of relevant Financial Sector Assessment Program (FSAP) missions by the IFIs and the date for the Plenary discussion of the MER will be maintained. In addition, the APG Secretariat will confirm the date of the on-site visit in consultation with the authorities of the member being evaluated. Any proposed changes to the year in which the on-site is scheduled will require Plenary approval, but not the date of the on-site as long as it remains within the approved year.

14. The considerations underlying the sequence of evaluations are:

- The sequence of evaluations followed in the second round of evaluations;
- Members' views on their preferred date - members are consulted on the possible dates for on-site visits and Plenary discussion of their MER, and this is taken into account in the schedule;
- The scheduled date of any possible FSAP mission – see section VIII below regarding the timing of the FSAP and of a mutual evaluation;
- The date of the last mutual evaluation or IFI assessment.

IV. Procedures and steps in the evaluation process

15. A summary of the key steps for the assessment team and the assessed member in the APG mutual evaluation process is set out at Appendix 1. Those steps are described more fully below.

Preparation for the on-site visit

16. At least six months before the on-site visit, and in consultation with the member, the Secretariat will finalise the timelines for the whole evaluation process. This will include the dates for the evaluation on-site visit and will be based on the timelines in Appendix 1 (some flexibility is permissible). The member being evaluated should indicate an identified contact person(s) or point(s) for the assessment, including logistics and planning.

17. The onus is on the member to demonstrate that it has complied with the Standards and that its AML/CFT regime is effective. The member should, therefore, provide all relevant information to the assessment team during the course of the assessment. As appropriate, assessors should be able to request or access documents (redacted if necessary), data and other relevant information.

18. All updates and information should be provided in an electronic format and members should ensure that laws, regulations, guidelines and other relevant documents are made available in English and the original language.

(a) Information Updates on Technical Compliance

19. The updates and information provided by the assessed member will provide key information that will enable the preparatory work to be carried out prior to the on-site visit. This preparatory work includes understanding the member's money laundering (ML) and terrorist financing (TF) risks, identifying potential areas of increased focus for the on-site (through a scoping exercise), and preparing the draft MER. Members should provide the necessary updates and information to the Secretariat no less than six months before the on-site visit. Prior to that, it would be desirable to have informal engagement between the member and the Secretariat.

20. For some members, AML/CFT issues are matters that are addressed not just at the level of the national government, but also at state/provincial or local levels. Members will need to indicate the AML/CFT measures that are the responsibility of state/provincial/local level authorities and provide an appropriate description of these measures. Assessors should also be aware that AML/CFT measures may be implemented at one or more levels of government. Assessors should therefore examine and take into account all the relevant measures, including those taken at a state/provincial/local level. Equally, assessors should take into account and refer to supra-national laws or regulations that apply to a member.

21. Members should rely on the questionnaire for the technical compliance update (see Appendix 3(a)) to provide relevant information to the assessment team. Along with the previous MER and follow-up reports, this will be used as a starting basis for the assessment team to conduct the desk-based review of technical compliance. The questionnaire is a guide to assist members to provide relevant information in relation to: (i) background information on any new or amended laws, regulations or guidance, and relevant updates and information on the institutional framework; (ii) information on risks and context; (iii) information on the measures that the member has taken to meet the criteria for each Recommendation.

22. Members should complete the technical compliance questionnaire carefully, including indicating in any relevant areas where nothing has changed in their AML/CFT regime since the previous MER. A member may also choose to present other additional information in whatever manner it deems to be most expedient or effective.

(b) Information on Effectiveness

23. Members should provide information on effectiveness based on the 11 Immediate Outcomes set out in the 2013 Assessment Methodology no less than four months before the on-site. Members should set out fully how each of the core issues, as set out in each Immediate Outcome, is being addressed. It is important for members 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. An example, to be used on a voluntary basis by members, of how to present the effectiveness information is contained in Appendix 3(b).

(c) Composition and Formation of Assessment Team

24. Assessors are initially selected by the APG Secretariat. This will normally take place at least six months before the on-site, and will be coordinated with any member that had earlier volunteered assessors for the proposed assessment. The APG Secretariat will submit the list of assessors to the

member undergoing the evaluation for information and comment before the visit. Any requests for changes to the composition of the team will be taken into account, but the final decision concerning the composition of the team will rest with the APG Secretariat.

25. An assessment team will usually consist of at least four expert assessors (comprising at least one legal, financial[1] and law enforcement expert), principally drawn from APG members, and will also include members of the APG Secretariat. Depending on the member and the ML and TF risks, additional assessors or assessors with specific expertise may also be required. In selecting the assessors, a number of factors will be considered: (i) their relevant operational and assessment experience; (ii) nature of the legal system (civil law or common law) and institutional framework; and (iii) specific characteristics of the jurisdiction (e.g. size and composition of the economy and financial sector, geographical factors, and trading or cultural links), to ensure that the assessment team has a suitable balance of knowledge and skills. Assessors should be very knowledgeable about the FATF Standards, and are required to attend an assessor training workshop on the 2013 Assessment Methodology before they undertake the on-site visit and conduct a mutual evaluation. Usually, at least one of the assessors should have had previous experience conducting an evaluation.

26. In joint evaluations, the assessment team will be made up of assessors and Secretariat staff from both the APG and the FATF/other FSRB/GIFCS as appropriate (see section VI). For some other APG evaluations, the APG Secretariat could, with the consent of the assessed member, invite an expert (member or Secretariat) from another FSRB, GIFCS, FATF, or the IMF/World Bank [2] to participate as an expert on the assessment team, on the basis of reciprocity. Further, in certain circumstances, an expert may be invited from a non-AML/CFT assessment body. Normally there should be no more than one, or in exceptional cases two, such experts per evaluation from other bodies on the assessment team.

27. Where appropriate, the APG Secretariat may also select an additional assessor to form part of the assessment team for developmental purposes. Such an assessor will normally be an expert who has not previously participated in a mutual evaluation or be from a member that has not previously been involved in a mutual evaluation.

28. Due to the nature of the peer review process, the Secretariat will work to ensure that the mutuality of the process is maintained, and members should provide qualified experts. Members with greater capacity should provide more assessors. A list of members' contribution of assessors for evaluations under the APG's third round will be maintained and monitored by the Secretariat and distributed to members and observers for information at the Annual Meeting.

(d) Responsibilities of Assessment Team

29. The core function of the assessment team is, collectively, to produce an independent report (containing analysis, findings and recommendations) concerning the member's compliance with the FATF standards, in terms of both technical compliance and effectiveness. A successful evaluation of an AML/CFT regime requires, at a minimum, a combination of financial, legal and law enforcement expertise, particularly in relation to the assessment of effectiveness. Experts therefore have to conduct an evaluation in a fully collaborative process, whereby all aspects of the review are conducted

[1] The assessment team should have assessors with expertise relating to the preventive measures necessary for the financial sector and designated non-financial businesses and professions.

[2] Participation (on a reciprocal basis) of experts from other observers that are conducting assessments, such as UNCTED, could be considered on a case by case basis.

holistically. Each expert is expected to contribute to all parts of the review, but should take the lead on, or take primary responsibility for, topics related to his or her own area of expertise.

30. The exact division of responsibilities will depend on the size and makeup of the assessment team, and the specific expertise of each assessor. However, an example of the division of primary responsibilities that may apply is as follows:

- *Technical Compliance*:
  - Legal: R.3, R.4, R.5 to R.7, R.24 and R.25, R.36 to R.39,
  - Financial: R.9 to R.19, R.26 and R.27, R.22 and R.23, R.28, R.35
  - Law Enforcement: R.20 and R.21, R.29, R.30 to R.32
  - All: R.1 and R.2, R.33 and R.34, R.8, R.40
- *Effectiveness:*
  - Legal: IO.2, IO.5, IO.7, IO.8, IO.9[3]
  - Financial: IO.3, IO.4
  - Law Enforcement: IO.6, IO.7, IO.8, IO.9
  - All / Other: IO.1, IO.10, IO.11

31. It is also important that assessors are able to devote their time and resources to reviewing all the documents (including the information updates on technical compliance, and information on effectiveness), raising queries prior to the on-site, preparing for and conducting the assessment, drafting the MER, attending the meetings (e.g. on-site visit, face-to-face meeting, and Plenary discussion), and adhere to the deadlines indicated.

32. The mutual evaluation is a dynamic and continuous process. The assessment team/Secretariat will engage and consult the assessed member on an ongoing basis, commencing at least six months before the on-site visit. Throughout the process the Secretariat will ensure that the assessors have access to all relevant material.

(e) Desk-Based Review of Technical Compliance

33. Prior to the on-site visit, the assessment team will conduct a desk-based review of the member's level of technical compliance, and the contextual factors and ML/TF risks. The review will be based on information provided by the member in the questionnaire/information updates on technical compliance, pre-existing information drawn from the member's second round MER, follow-up reports and other credible or reliable sources of information. This information will be carefully taken into account, though the assessment team can also review the findings from the previous MER and follow-up reports and may highlight relevant strengths or weaknesses not previously noted. If the assessment team reach a different conclusion to previous MERs and follow-up reports (in cases where the Standards and the relevant laws, regulations or other AML/CFT measures have not changed) then they should explain the reasons for their conclusion.

34. Subsequent to the review, the assessment team will provide the member with a first draft of the technical compliance annex (which needs not contain ratings or recommendations) approximately three months before the on-site visit. This will include a description, analysis and list of potential

[3] IO.7 to IO.9 may be assessed jointly by the legal and law enforcement assessors.

technical deficiencies. The member will have one month to clarify and comment on this first draft on technical compliance.

35. In conducting the assessment, assessors should only take into account relevant laws, regulations or other AML/CFT measures that are in force and effect at that time, or will be in force and effect by the end of the on-site visit. Where relevant bills or other specific proposals to amend the system are made available, these will be referred to in the MER (including for the purpose of the recommendations to be made to the member) but will not be taken into account for ratings purposes.

(f) Ensuring Adequate Basis to Assess International Cooperation

36. Six months before the on-site visit, APG members, the FATF and FSRBs[4] will be invited to provide information on their experience of international co-operation with the member being evaluated. Information on international cooperation should be provided at least 3 months before the on-site.

37. In addition, the assessment team and the member may also identify and seek specific feedback from key jurisdictions to which the assessed member has provided international cooperation, or from which it has requested it. The feedback could relate to: (i) general experience, (ii) positive examples, and (iii) negative examples, of the assessed member's level of international cooperation. The responses received will be made available to the assessment team and the assessed member.

(g) Identifying Potential Areas of Increased Focus for On-Site Visit – Scoping Note

38. To support the assessment of effectiveness in relation to the 11 Immediate Outcomes, prior to the on-site visit the assessment team may identify specific areas to which it would pay more attention during the on-site visit and in the MER. This is based on the team's preliminary analysis of both technical compliance and effectiveness issues and will usually relate to effectiveness issues but could also include technical compliance issues. In doing so, the team will consult the member and, as outlined below, the scoping note prepared by the team will be reviewed by a quality and consistency review team. In addition, APG and observer delegations will be invited to provide any comments that they may have that would assist the team to focus on areas of higher risk that need increased focus.

39. Where there are potential areas of increased focus for the on-site visit, the assessment team should obtain and consider all relevant information and commence discussion of these areas approximately 4-6 months before the on-site, and consult the member at least two months before the on-site. The member should normally provide additional information regarding the areas for increased focus. While the prerogative lies with the assessment team, the areas for increased focus should, to the extent possible, be mutually agreed with the member and should be set out in a draft scoping note. The scoping note should set out briefly (in no more than two pages) the areas for increased focus and why these areas have been selected. The draft scoping note, along with relevant background information (e.g. the member's risk assessment(s)), should be sent to the reviewers (described in the section on quality and consistency, below) and to the member two months before the on-site visit.

40. Reviewers should, within two weeks of receiving the scoping note, provide their feedback to the assessment team regarding whether the scoping note reflects a reasonable view on the focus of the assessment, having regard to the material made available to them as well as their general knowledge of the member. The assessment team should consider the merit of the reviewers' comments, and amend the scoping note as needed, in consultation with the member. The final version should be sent to the

[4] FATF and FSRBs and their members will only be invited to provide this information where they are willing to reciprocally invite APG members to provide the same type of information in relation to their mutual evaluations.

member at least three weeks prior to the on-site visit, along with any requests for additional information on the areas of increased focus. The member should seek to accommodate any requests arising from the additional focus.

41. To expedite the mutual evaluation process, and to facilitate discussions on-site, one week before the on-site visit the assessment team will share with the member being assessed a revised draft TC annex, draft TC text for MER and an outline of initial findings/key issues to discuss on effectiveness.

(h) Programme for On-Site Visit

42. The member (designated contact) should work with the Secretariat and prepare a draft programme and coordinate the logistics for the on-site visit. The draft programme, together with any specific logistical arrangements, should be worked on two months prior to the on-site and finalised with the assessment team no later than two weeks before the visit. Appendix 2 is a list of authorities and businesses that would usually be involved in the on-site visit. The assessment team may also request additional meetings during the on-site visit.

43. The draft programme should take into account the areas where the assessment team may want to apply increased focus. Where practical, meetings could be held in the premises of the agency/organisation being met since this allows the assessors to meet the widest possible range of staff and to obtain information more easily. However in some circumstances it may be warranted for meetings to be held at one venue or just a few venues per day. This may be due to travel time between venues, security challenges and the availability of suitable premises.

(i) Confidentiality

44. All documents and information produced: (i) by an assessed member during a mutual evaluation exercise (*e.g.* updates and responses, documents describing a member's AML/CFT regime, measures taken or risks faced (including those for which there will be increased focus), or responses to assessors' queries); (ii) by the APG Secretariat or assessors (*e.g.* reports from assessors, draft MER); and (iii) comments received through the consultation or review mechanisms, should be treated as confidential. They should only be used for the specific purposes provided and not be made publicly available, unless the assessed member and the APG (and where applicable, the originator of the document) consents to their release. These confidentiality requirements apply to the assessment team, the Secretariat, reviewers, officials in the assessed member and any other person with access to the documents or information. In addition, prior to the on-site visit the members of the assessment team and reviewers should sign a confidentiality agreement, which will include text regarding the need to declare a conflict of interest.

On-site visit

45. The on-site visit provides the best opportunity to clarify issues relating to the member's AML/CFT system. Assessors need to be fully prepared to review the 11 Immediate Outcomes relating to the effectiveness of the system and clarify any outstanding technical compliance issues. Assessors should also pay more attention to areas where higher money laundering and terrorist financing risks are identified. Assessors must be cognisant of different members' circumstances and risks; and that members may adopt different approaches to meet the FATF Standards and to create an effective system. Assessors thus need to be open and flexible and seek to avoid narrow comparisons with their own national requirements.

46. Experience has shown that at least 7-8 days of meetings is required for members with developed AML/CFT systems. A typical on-site visit could thus allow for the following:

- An initial half day preparatory meeting between the Secretariat and assessors.
- 7-8 days of meetings[5] with representatives of the member (both public and private sector), including an opening and closing meeting. Time may have to be set aside for additional or follow-up meetings, if, in the course of the set schedule, the assessors identify new issues that need to be explored, or if they need further information on an issue already discussed.
- 1-2 days where the Secretariat and assessors work on the draft MER, ensure that all the major issues that arose during the evaluation are noted in the report, and discuss and agree on preliminary ratings, and key recommendations. The assessment team should provide a written summary of its key findings to the assessed member officials at the closing meeting.

47. The total length of the mission for a normal evaluation is therefore likely to be in the order of 10 working days, but this could be extended for large or complex jurisdictions.

48. It is important that the assessment team be able to request and meet with all relevant agencies during the on-site. The member being evaluated, and the specific agencies met, should ensure that appropriate staff are available for each meeting. While the level and type of officer required will vary from agency to agency, generally speaking members should ensure that both senior managers, who can 'speak for' the agency/jurisdiction at a policy level, as well as 'operational' staff who can if necessary answer detailed questions on AML/CFT implementation, are present at each meeting. Agencies should be made aware by the member that they may be asked quite detailed and probing questions. The persons present should therefore be familiar with the content of the member's TC and effectiveness responses, especially as it relates to their area of expertise, and be prepared for detailed questions relating to that response.

49. Other than for transportation and interpretation purposes, there may be no need for a dedicated officer to 'escort' the assessment team during its meetings, though this can be helpful. If the coordinating agency wishes to have an officer attend meetings with the team, the officer will do so as an observer and their inclusion will be at the discretion of the assessment team.

50. Meetings with the private sector or other non-government representatives[6] are an important part of the visit and, generally, the assessors should be given the opportunity to meet with such bodies or persons in private, without a government official present, if there is concern that the presence of the officials may inhibit the openness of the discussion. . The team may also request that meetings with certain government agencies are restricted to those agencies only.

51. Where English is not an official language of the assessed member, the process of translation of relevant laws, regulations and other documents should start at an early stage, so that they can be provided to the assessment team in a timely fashion e.g. English translation of the TC update and relevant laws, regulations etc. must be provided at least six months before on-site, and the effectiveness response including relevant documents (court cases) at least four months before the on-site. However, the assessment team should also be provided with the relevant laws or other documents in the language of the member, since translations of technical texts are not always perfect. During the on-site visit there also needs to be professional and well prepared interpreters if the member's officials are not fluent in English. The member being evaluated will need to provide interpreters.

[5] The assessment team should also set aside time midway through the on-site to review the progress of the mutual evaluation and where relevant, the identified areas of increased focus for the on-site initially.

[6] E.g. those listed in Appendix 2.

52. It is the responsibility of the member being evaluated to provide necessary security and transportation arrangements. All transportation during the visit, both to and from the airport and between appointments, is the responsibility of the member under review.

53. The assessment team should be provided with a dedicated office for the duration of the on-site visit. The room should have photocopying, printing and other basic facilities, as well as internet access.

54. Lunches should be scheduled to be kept relatively short and, if necessary, working lunches may be arranged. Formalities should be dispensed with to the extent possible during the visit. For example, formal dinners should be kept to a minimum.

55. Gift giving to the assessment team should be avoided, and any gifts, if provided, should be of low monetary value.

Post on-site - preparation of draft Executive Summary and MER

56. There should be an adequate amount of time, normally 25 weeks, between the end of the on-site visit and the discussion of the MER in Plenary. The timely preparation of the MER and Executive Summary[7] will require the assessors to work closely with the Secretariat and the member. The time period may also be extended or adjusted and based on justified circumstances (and with the consent of the assessed member), a shorter period of time may be allowed for.

57. The steps in finalising a draft report for discussion at Plenary, and the approximate time that is required for each part, are set out in greater detail below (see also Appendix 1).

(j) 1st Draft MER

58. The assessment team will have six weeks to coordinate and refine the 1st draft MER (including the key findings, potential issues of note and priority recommendations to the member). The 1st draft MER will include the preliminary recommendations and ratings. This is then be sent to the member for comment. The member will have four weeks to review and provide its comments on the 1st draft MER to the assessment team. During this time, the assessment team should be prepared to respond to queries and clarifications that may be raised by the member.

(k) 2nd Draft MER and Executive Summary

59. On receipt of the member's comments on the 1st draft MER, the assessment team will have two weeks to review the comments and make further amendments, as well as prepare the Executive Summary. The 2nd draft MER and Executive Summary will be then be sent to the member and to the reviewers (approximately 12 weeks after the on-site).

(l) Quality & Consistency Review

60. As part of the APG mutual evaluation process, there will be a quality and consistency review. A quality and consistency review team will be formed for each mutual evaluation and will have the role of reviewing the scoping note before the on-site (per section IV(g) above), and the 2nd draft of the MER approximately 12 weeks after the on-site.

[7] The format for the Executive Summary and MER is contained in Annex II of the Methodology. Assessors should also pay attention to the guidance on how to complete the Executive Summary and MER, including with respect to the expected length of the MER (100 pages or less, together with a technical annex of up to 60 pages).

61. The main functions of the reviewers are to ensure MERs are of an acceptable level of quality and consistency; and to assist the assessment team by reviewing and providing timely input on the scoping note and the draft MER and Executive Summary (including any annexes) with a view to:

    - Commenting on assessors' proposals for the scope of the on-site, including on whether the assessors' draft scoping note reflects a reasonable view on the focus of the assessment.
    - Reflecting a correct interpretation of the FATF Standards and application of the 2013 Assessment Methodology (including the assessment of risks, integration of the findings on technical compliance and effectiveness and areas where the analysis and conclusions are identified as being clearly deficient).
    - Checking whether the description and analysis supports the conclusions (including ratings); and whether, based on these findings, sensible priority recommendations for improvement are made.
    - Where applicable, highlighting potential inconsistencies with earlier decisions adopted by the FATF and APG on technical compliance and effectiveness issues.
    - Checking that the substance of the report is generally coherent and comprehensible.

62. The quality and consistency review process will be conducted through the APG's Mutual Evaluation Working Group (MEWG). The MEWG will form a quality and consistency review team for each mutual evaluation. The APG Secretariat/MEWG will invite qualified volunteer experts from APG members and observers to participate in review teams. Qualified volunteer experts (e.g. trained in the 2013 Assessment Methodology) will include experts from members and Secretariats of the APG, FATF, other FSRBs, GIFCS, and staff of the IFIs and other observer organisations.

63. To avoid potential conflicts of interest, the reviewers selected for any given quality and consistency review will be from members other than those of the assessors, and will be made known to the member and assessors in advance. Generally, at least three reviewers will be allocated to each assessment; comprising at least two reviewers from the APG and at least one reviewer from the FATF, another FSRB, GIFCS, the IMF/World Bank or other observer organisations, each of whom could in principle focus on part of the report. The Secretariat will determine the final make-up of each review team.

64. The reviewers will need to be able to commit time and resources to review:

    (i) the scoping note, and

    (ii) the quality, coherence and internal consistency of the 2nd draft MER, taking into account consistency with the FATF Standards and APG and FATF precedents. In doing so, the reviewers should have a copy of the comments provided by the member on the 1st draft MER.

65. As noted in paragraph 40 above, the reviewers will have two weeks to examine the scoping note and provide their comments to the APG Secretariat for dissemination to the assessment team. The assessment team will consider the merit of the reviewers' comments, and amend the scoping note as needed, in consultation with the member.

66. The reviewers will have two weeks to examine the 2nd draft MER and provide their comments to the APG Secretariat for dissemination to the assessment team. Following the receipt of the reviewers' comments, the assessment team will consider those comments and prepare a 3rd draft MER and Executive Summary. The 3rd draft MER will be sent to the assessed member for comment as part of the ongoing process of preparing and finalising the MER.

67. The reviewers for the quality and consistency review do not have any decision making powers or powers to change a report. It is the responsibility of the assessment team to consider the reviewers' comments and then decide whether any changes should be made to the report.

68. The assessment team will provide a short response to the reviewers on the decisions that it has made and the changes it has made to the report based on the reviewers' comments.

69. To ensure transparency, all comments from the reviewers will be disclosed to the assessors and member. The reviewers' comments on the 2nd draft MER, and the assessment team's response, will be circulated by the Secretariat at the same time as the final draft MER is distributed to members and observers (five weeks prior to the Annual Meeting). This will help to identify in a transparent manner possible issues for discussion and will inform delegations as they provide written comments on the draft MER.

70. Due to the nature of the peer review process, the Secretariat will work to ensure that the mutuality of the process is maintained. To assist with this, members and observers should provide qualified experts as reviewers. A list of past and forthcoming reviewers will be maintained and monitored by the Secretariat and circulated to members and observers for information at the Annual Meeting.

(m) Face-to-face Meeting

71. The assessment team and assessed member should work to resolve any disagreements over the content of the 3rd draft MER before it is circulated to members and observers for consideration five weeks before the Annual Meeting. Resolution of any areas of disagreement should, to the extent possible, not be left to the margins of the Annual Meeting as late amendments to the draft MER would preclude proper Plenary discussion and consideration of the draft MER.

72. A face-to-face meeting is an important way to assist the member and assessment team to resolve outstanding issues.

73. If there are significant disagreements over technical compliance or effectiveness issues, as identified either by the assessed member or assessment team, a face-to-face meeting should ideally be held at least 8 weeks before the Annual Meeting (via video or tele-conference if needed), depending on the need and other considerations e.g. travel costs and availability of assessment team members. If not conducted by video or tele-conference, the face-to-face meeting would normally be held in the assessed jurisdiction, but it could be held elsewhere at a location to be mutually agreed by the assessment team and assessed member. Participation will be on a self-funded basis. If there is a need for a face-to-face meeting, at least 6 weeks' notice should be given to all parties involved.

74. During this session, the assessment team and member should work to resolve any remaining disagreements over technical compliance or effectiveness issues and the priority issues for Plenary discussion. The member should provide any additional comments and material in writing to the assessment team at least one week prior to the meeting.

75. A face-to-face meeting can also be held in the margins of the Annual Meeting shortly before Plenary discussion of the MER (normally on the weekend immediately prior to the Annual Meeting). However, such meetings will normally discuss only the mechanics and process for adoption of the report, not substantive issues, and the draft MER will not be subject to further change before the Plenary discussion. In exceptional circumstances and only for very limited sections of the MER, however, based on APG members' or observers' comments on the draft report (see next section) and the outcomes of further discussions between the assessment team and the member, the member and the team may prepare an addendum, a hard copy of which will be circulated to APG members and

observers prior to the Plenary's consideration of the MER during the Annual Meeting. This should however be avoided and issues should be resolved, if possible, before the circulation of the final draft MER 5 weeks before the Annual Meeting.

(n) Identifying Issues for Plenary Discussion

76. The revised Executive Summary and MER (final draft), together with the conclusions of the quality and consistency review mechanism, assessors' responses and assessed member's formal response to the final draft MER, will be sent to all members and observers at least five weeks prior to Plenary for their comments. Delegations and reviewers will have three weeks to provide any written comments on the MER and Executive Summary and, in particular, to identify any specific issues that they wish to discuss in Plenary. The comments should focus on the key substantive issues, or on other high level or horizontal aspects of the assessment, though other observations may also be made. The comments received will be made available to all delegations.

77. Based on the MER and Executive Summary, and comments received, the Secretariat will engage the member and assessment team and reviewers and prepare a list of (usually 5 to 7) priority and substantive issues that will be discussed in Plenary. This should take into account the issues that the assessed member and delegations are most keen to discuss. The list of priority issues for discussion in Plenary would include key issues arising from the report (whether referenced by the member, the assessment team or delegations), as well as any areas of possible inconsistency or interpretation with other MERs adopted by the APG. Examples of priority issues are: key ML risks, ratings, interpretation of laws and standards, findings on effectiveness, core MER recommendations. If needed, the Secretariat will consult with the MEWG Co-Chairs before finalising the list of issues. The Secretariat will circulate the finalised list of priority issues to delegations one week before the Plenary discussions.

(o) Respecting Timelines

78. The timelines are intended to provide guidance on what is required if reports are to be prepared within a reasonable timeframe and in sufficient time for discussion in Plenary. It is therefore important that both the assessors and the member respect the timelines.

79. Delays may significantly affect the ability of the Plenary to discuss the report in a meaningful way. The draft schedule of evaluations has been prepared so as to allow enough time between the on-site visit and the Plenary discussion. A failure to respect the timetables may mean that this would not be the case. By agreeing to participate in the mutual evaluation process, the member and the assessors undertake to meet the necessary deadlines and to provide full, accurate and timely responses, reports or other material as required under the agreed procedure. Where there is a failure to comply with the agreed timelines, then the following actions could be taken (depending on the nature of the default):

    a) Failure by the member to provide a timely or sufficiently detailed response to the TC update, or response on the core issues on effectiveness, could lead to deferral of the mutual evaluation – the Executive Secretary or the APG Co-Chairs may write to the member's Primary Contact Point or relevant Minister. APG members are to be advised as to the reasons for the deferral and publicity could be given to the deferment (as appropriate).

    b) Failure by the member to provide a timely response to the draft MER – the Executive Secretary or the APG Co-Chairs may write a letter to the member's Primary Contact Point or relevant Minister. Where the delay results in a report not being discussed at the next Annual Meeting, members are to be advised of the reasons for deferral. APG members may consider whether the deferral amounts to a breach of APG membership requirements and what action, if any, may need to be taken.

c) Failure by the assessors to provide timely or sufficiently detailed reports or responses at any stage of the mutual evaluation process – the Executive Secretary or the APG Co-Chairs may write a letter to the Primary Contact Point for the member, or organisation, from which the assessor has come.

d) Failure by the reviewers to provide timely comments on the risk scoping and draft MER – the Executive Secretary or the APG Co-Chairs may write a letter to the Primary Contact Point for the member, or organisation, from which the reviewer has come.

e) Failure by the Secretariat to provide timely reports at any stage of the mutual evaluation process – the APG Co-Chairs may liaise with the Executive Secretary.

80. The Secretariat will keep the APG Co-Chairs advised of any failures so that the APG Co-Chairs can respond in an effective and timely way. The Plenary is also to be advised if the failures result in a request to delay the discussion of the MER.

(p) The Plenary Discussion

81. The discussion of each MER and Executive Summary (particularly the list of priority issues)[8] will focus on high level and key substantive issues. Adequate time should always be set aside to discuss the member's response to the mutual evaluation and other issues, including any significant and unresolved disagreements. The discussion is likely, on average, to take two hours of Plenary time. The procedure for the discussion will be as follows:

- Assessment team briefly presents, in high level terms, the key issues and findings from the report. The team will have the opportunity to intervene/comment on any issue concerning the Executive Summary or MER.
- Assessed member makes a short opening statement.
- The Plenary discusses the list of priority issues identified. This would usually be introduced briefly by the Secretariat, with the assessors and the assessed member having the opportunity to provide additional information.
- Adequate time (approximately half the Plenary's time) will be set aside to discuss the overall situation of the assessed member's AML/CFT regime and ML/TF risks, the priority actions and recommendations set out in the Executive Summary, the member's response to the mutual evaluation, including on ratings and any actions already taken, and the key findings.
- Time permitting, other issues could be raised from the floor, and discussed by the Plenary.

82. All observers are permitted to attend discussions of APG mutual evaluation reports. Such representatives may participate by making comments, asking questions or suggesting changes to a draft MER but do not participate in the formal adoption of an MER, which is a matter for APG members only.

83. The FATF Secretariat's representative at the Plenary will be expected to assist and advise on all issues relating to the interpretation of the Recommendations and the quality and consistency aspects of the draft MER. The Plenary discussion will provide members and observers adequate opportunity to raise and discuss concerns about quality and consistency of an MER.

[8] The Executive Summary will describe the key risks, the strengths and weaknesses of the system, and the priority actions for the member to improve its AML/CFT regime.

(q) *Adoption of the MER and Executive Summary*

84. At the end of the Plenary discussion, the MER and the Executive Summary will be submitted to Plenary for adoption. Prior to the formal adoption of the report, the Plenary should discuss the nature of the follow-up measures that are required (see section IX below).

85. The final report is a report of the APG and not simply a report by the assessors. As such, the Plenary will retain the final decision on the wording of any report, consistent with the requirements of the FATF Standards and Methodology. The Plenary will give careful consideration to the views of the assessors and the assessed member when deciding on the wording, as well as take into account the need to ensure consistency between reports.

(r) Publication and other Procedures following the Plenary

86. Following the discussion and adoption of the report at the Plenary meeting, the assessment team will amend all documents as necessary, including further checks for typographical or similar errors. The Secretariat will circulate a revised version of the report to the member within one week of the Plenary. Within two weeks of receipt of the final version of the MER from the Secretariat, the member must confirm that the MER is accurate and/or advise of any typographical or similar errors in the MER. Care will be taken to ensure that no confidential information is included in any published report.

87. As required under the ex-post review of major quality and consistency problems (see section X below), immediately following their adoption, and before publication, all MERs will be provided to the FATF Secretariat and all other assessment bodies for possible consideration in the Global Quality and Consistency Review process. Following completion of that process, all MERs and Executive Summaries will be published on the APG's website. Where there is no such review process then the reports should be published within six weeks of adoption.

V. Evaluations of Non Members

88. If agreed by the APG Plenary, in exceptional circumstances, the APG may also conduct or participate in an assessment of an APG observer jurisdiction. The procedures laid out in sections I to IV of these procedures will apply. If necessary, the APG Secretariat will coordinate arrangements with the Secretariat of another assessment body.

VI. Joint mutual evaluations with the FATF and other FSRBs or GIFCS

89. The FATF's policy is that FATF members that are also members of FSRB(s) will undergo a joint evaluation by these bodies. This is also the APG's policy. Generally, the FATF will be the principal organiser, and will provide three assessors, while 1-2 assessors will be provided by the participating FSRB(s). The FATF and the FSRB(s) Secretariats will participate. The first discussion of the MER should take place in the FATF and, given the additional measures adopted by the FATF for joint evaluations (outlined below), the general presumption is that the FATF's view would be conclusive.

90. The process (including the APG and FATF procedures for preparing the draft MER and Executive Summary) for joint evaluations are the same as for other APG evaluations, with the APG and its members having opportunities to participate directly through being part of the assessment team, and also being able to provide comments and input. The APG will allow reciprocal participation in mutual evaluation discussions for FATF members, and on this basis, the following measures will also apply for joint evaluations.

- A representative from the APG will be given a specific opportunity to intervene during the FATF Plenary discussion of the MER.
- All the FATF assessors on the assessment team are encouraged to attend the APG Plenary at which the joint evaluation report is considered, and at least one FATF assessor should attend the APG Plenary. The same approach should be applied to IFI-led assessments of joint APG/FATF members.
- In an exceptional case where a report was agreed within FATF but subsequently the APG identified major difficulties with the text of the report, then the APG Secretariat would advise the FATF Secretariat of the issues, and the issues should be discussed at the following FATF Plenary.
- Consideration will also be given to the timing of publication, if the MER has not been discussed in the APG, with a view to finding a mutually agreed publication date.

91. The APG will be able to undertake joint assessments with other FSRBs or GIFCS when an APG member is also a member of another FSRB or GIFCS, but not a FATF member. Where an APG member is a member of another FSRB or GIFCS, and not a FATF member, the principal organiser will either be the APG or the other FSRB or GIFCS, based on discussions between the joint member and the APG Secretariat, and the other FSRB or GIFCS Secretariat. The composition of the assessment team and the process for adoption of the MER and Executive Summary will be decided after close consultation between the joint member and the two Secretariats.

VII. IMF or World Bank led assessments of APG members

92. The APG is responsible for the mutual evaluation process for all of its members, and there is a presumption that the APG will conduct the mutual evaluations[9] of all APG members as part of this process. The presumption can be overridden at the discretion of the APG Plenary on a case by case basis, and with the evaluated member's agreement. For the purposes of the APG third round of mutual evaluations, the APG Plenary has discretion as to the number of APG evaluations that could be conducted by the IMF or World Bank (IFI). However, it is not expected that the IFIs would be permitted to conduct more than two APG evaluations in any given year.

93. For the APG assessment schedule to be finalised with appropriate certainty and in a coordinated manner, the process leading to the Plenary decision as to which APG members will have an assessment led by an IFI team should be clear and transparent. In order for the evaluation schedule to be appropriately planned and assessment teams to be formed in sufficient time, it will be necessary for the APG to be involved at an early stage in the process of determining which members will be assessed by an IFI. The FATF's ECG will be informed at every Plenary as to the current status of the IFIs assessment schedule. The IFIs are also expected to inform the APG Secretariat of any proposals to assess an APG member and the Plenary will decide on any such requests. Where the IMF or WB conduct an AML/CFT assessment as part of the APG third round they should use procedures and a timetable similar to those of the APG.

94. The APG Plenary will, in all cases, have to consider and adopt an IFI assessment that is conducted under the APG third round for it to be accepted as an APG mutual evaluation.

[9] Including any follow up that may be required.

VIII. Co-ordination with the FSAP process

95. The FATF Standards are recognised by the IFIs as one of twelve (12) key standards and codes, for which Reports on the Observance of Standards and Codes (ROSCs) are prepared, often in the context of a Financial Sector Assessment Programme (FSAP). Under current FSAP policy, every FSAP and FSAP update should incorporate timely and accurate input on AML/CFT. Where possible, this input should be based on a comprehensive quality AML/CFT assessment and, in due course, in the case of the APG, on an MER follow-up assessment, conducted against the prevailing standard. The APG and the IFIs should therefore co-ordinate with a view to ensuring a reasonable proximity between the date of the FSAP mission and that of a mutual evaluation or a MER follow-up assessment conducted under the prevailing methodology, to allow for the key findings of that evaluation or MER follow-up assessment to be reflected in the FSAP; and members are encouraged to co-ordinate the timing for both processes internally and with the APG Secretariat and IFI staff.[10]

96. The basic products of the evaluation process are the MER and the Executive Summary (for the APG) and the Detailed Assessment Report (DAR) and ROSC (for the IFIs)[11]. The Executive Summary, whether derived from an MER or MER follow-up assessment report, will form the basis of the ROSC. Following the Plenary, and after the finalisation of the Executive Summary, the summary is provided by the Secretariat to the IMF or World Bank so that a ROSC can be prepared following a pro forma review.

97. The substantive text of the draft ROSC will be the same as that of the Executive Summary, though a formal paragraph will be added at the beginning:

> "This Report on the Observance of Standards and Codes for the *FATF Recommendations and Effectiveness of AML/CFT Systems* was prepared by the Asia/Pacific Group on Money Laundering. The report provides a summary of [the/certain][12] AML/CFT measures in place in [*Jurisdiction*] as at [*date*], the level of compliance with the FATF Recommendations, the level of effectiveness of the AML/CFT system, and contains recommendations on how the latter could be strengthened. The views expressed in this document have been agreed by the APG and [*Jurisdiction*], but do not necessarily reflect the views of the Boards or staff of the IMF or World Bank."

[10] If necessary, the staff of the IFIs may supplement the information derived from the ROSC to ensure the accuracy of the AML/CFT input. In instances where a comprehensive assessment or follow-up assessment against the prevailing standard is not available at the time of the FSAP, the staff of the IFIs may need to derive key findings on the basis of other sources of information, such as the most recent assessment report, and follow-up and/or other reports. As necessary, the staff of the IFIs may also seek updates from the authorities or join the FSAP mission for a review of the most significant AML/CFT issues for the country in the context of the prevailing standard and methodology. In such cases, staff would present the key findings in the FSAP documents; however, staff would not prepare a ROSC or ratings.

[11] The DAR uses a similar template to that of the common agreed template that is annexed to the Methodology and has a similar format.

[12] For ROSCs based on an MER, the word "the" should be used; for ROSCs based on a MER follow-up assessment, the alternative wording "certain" would be used (since the follow-up assessment is not a comprehensive one)

IX. Follow-up process

98. As an Associate Member of the FATF, the APG is required to have follow-up procedures similar to those of the FATF. These procedures are based on the FATF's universal procedures and fourth round procedures, but have been adapted to suit the specific needs and nature of the APG's diverse membership and current levels of implementation in the region, and bearing in mind practical/resource considerations.

99. The APG's follow-up process is intended to: (i) encourage members' implementation of the FATF Standards; (ii) provide regular monitoring and up-to-date information on members' compliance with the FATF Standards (including the effectiveness of their AML/CFT systems); (iii) apply sufficient peer pressure and accountability; and (iv) better align the APG and FSAP assessment cycle.

Key principles

100. The key principles of effective follow-up procedures include:

i. Rectify MER deficiencies: Follow-up should require evaluated members to rectify the deficiencies identified in the MER and to implement the recommendations made.

ii. Graduated Steps: There should be mechanisms to encourage compliance with the FATF Recommendations include regular progress reporting and a set of enhanced follow-up measures, including expedited reporting, if needed.

iii. Flexibility: Members with more robust AML/CFT systems and fewer NC/PC ratings for technical compliance and fewer low/moderate ratings for effectiveness in their MER are subject to less onerous processes that exert less pressure, and vice-versa.

iv. Risk-based: A risk-based approach will be taken, bearing in mind the size and nature of the APG membership, time and resource considerations, and the overall ML/TF risk posed by a member, to focus more attention on those members that have significant deficiencies.

v. Criteria for Enhanced Follow-Up: The Plenary's decision on whether to place members on enhanced follow-up, at the time of adoption of the MER, will be determined by the number of NC/PC ratings for technical compliance and the number of low or moderate ratings for effectiveness. However, the criteria for being placed under or exiting from enhanced follow-up, at any stage of the follow-up process after the adoption of the MER, will be primarily based on a qualitative analysis of the progress made by the member against priority recommended actions in its MER, as well as the level of technical compliance and effectiveness.

vi. No desk-based re-rating of effectiveness: There will be no re-rating for effectiveness of any of the 11 Immediate Outcomes as part of the follow-up reporting process. Re-rating for effectiveness is possible only as part of the follow-up assessment conducted about five years after adoption of the MER (see xii below).

vii. Re-ratings for technical compliance**:** Re-ratings for technical compliance [to Largely Compliant or Compliant] on any one or more of the 40 FATF Recommendations will be possible upon request by the assessed member, or if deemed appropriate under the circumstances. It is not expected that there will be any re-rating if the member has not addressed underlying key deficiencies, e.g. new laws or regulations not issued and/or in effect, new procedures or other measures not implemented, etc.

viii. Secretariat/Team analysis: Follow-up reports by members should be analysed by the Secretariat or an APG follow-up review team, i.e. a small team of experts from APG members and

observers drawing on former assessment team members whenever possible. Only an APG review team can undertake a re-rating for technical compliance.

ix. Recommendations to Plenary: Analysis reports, either by the Secretariat or an APG review team, should highlight both progress made and remaining deficiencies, and include recommendations to members regarding the mode of future follow-up and associated measures.

x. Mutual Evaluation Working Group (MEWG) Review: All progress and analysis reports pertaining to members under enhanced follow-up, re-rating for technical compliance, or recommending a change in the category of follow-up, will be submitted to the MEWG for consideration and endorsement in the first instance.

xi. Referral to Steering Group: If the deficiencies identified in the analysis report are serious enough to warrant consideration of any membership action under the Graduated Steps (refer paragraph 118 below), the MEWG may at any time refer the matter and any recommendations to the APG Steering Group.

xii. Follow-Up On-Site Assessment: There will be a follow-up assessment which should take place within a reasonable timeframe (normally 5 years) after the adoption of the MER. This will involve an on-site visit of 2-3 days. Re-ratings on both TC and effectiveness are possible.

xiii. Publication: Regular follow-up reports and their analysis made by the Secretariat/Review Team, as well as follow-up on-site assessment reports will be published. The Plenary will retain flexibility on the frequency with which enhanced follow-up reports are published. At a minimum enhanced follow-up reports will be published whenever there is a re-rating.

Modes of follow-up

101. Members may, at any stage, including following the discussion and adoption of a MER, decide to place a member under either regular or enhanced follow up:

i. Regular follow-up is the default monitoring mechanism, and is based on a system of biennial reporting.

ii. Enhanced follow-up is based on the APG's membership policy and deals with members with significant deficiencies (for technical compliance or effectiveness) in their AML/CFT systems through a more intensive process of follow up.

(a) Regular Follow-up

102. Regular follow-up will be the default mechanism to ensure a continuous and ongoing system of monitoring. This is the minimum standard that will apply to all members. Members subject to regular follow-up will report back to the Plenary every two years.

103. **Biennial Reporting**: The assessed member will provide a follow-up report to the Secretariat by 31 January on a biennial basis after adoption of the MER setting out the actions it has taken since adoption. This should include relevant changes to the laws, regulations, guidance, relevant data and information relating to effectiveness, as well as other contextual and institutional information. The expectation is that satisfactory progress would have been made.

104. **Secretariat/ Review Team analysis**: The member's progress report will be analysed either by the Secretariat or by an APG Review Team comprised of experts from APG members and observers (drawing on former assessment team members whenever possible), as follows:

- Secretariat: Where there are no re-ratings of technical compliance, the Secretariat will prepare an analysis report.

- Review Team: A Review Team will conduct the analysis where there is a re-rating/possible re-rating for technical compliance [to Largely Compliant or Compliant] either when requested by the member, or arising from a preliminary Secretariat review.

105. **Analysis Report**: This is a desk-based review, however to the extent possible issues relating to effectiveness will also be considered. *Examples* of substantive issues to be considered in the analysis report include:

- Significant changes in the member leading to a decline or improvement in technical compliance or effectiveness.
- Insufficient progress made by the member against the priority actions in its MER.
- The analysis report involves re-rating [to Largely Compliant or Compliant] for any one or more of the FATF 40 Recommendations (Review Team only).
- The report recommends placing the member on enhanced follow-up.

106. When preparing the analysis report for Plenary, the Secretariat/Review Team may consult the original assessors, if available. The analysis report should be provided to the assessed member for comments before it is sent to other APG members. The analysis report will contain a recommendation(s) regarding the next step in the follow-up process.

107. **MEWG**: All analysis reports and associated progress reports that involve re-rating for technical compliance or proposals to change the mode of follow-up (i.e. from regular to enhanced follow-up) will be submitted to the MEWG for consideration and endorsement in the first instance, before being submitted to members for adoption at the Annual Meeting.

108. **Plenary**: The Plenary will consider the analysis report and progress report; the overall progress made by the member; and decide whether the member should report back on a regular basis, or should be placed on enhanced follow-up and report back sooner. In deciding on the category of follow-up, the Plenary will give consideration to the key issues discussed in the analysis report, i.e. any decline in technical compliance or effectiveness or insufficient progress made.

(b) Enhanced Follow-up

109. The Plenary may decide at its discretion, either when a member's MER is adopted or at any other time, that the member should be placed on enhanced follow-up. This will result in the member reporting back more frequently than for regular follow-up, and may also involve other measures being taken under the **Graduated Steps** (refer paragraph 118 below).

110. **Criteria**: In deciding whether to place a member on enhanced follow-up, the Plenary will consider the following factors:

a) After the discussion of the MER: a member will be placed immediately on enhanced follow-up if any one of the following applies:

(i) it has eight or more NC/PC ratings for technical compliance, or

(ii) it is rated NC/PC on any one or more of R.3, 5, 10, 11 and 20, or

(iii) it has a low or moderate level of effectiveness for seven or more of the 11 effectiveness outcomes, or

(iv) it has a low level of effectiveness for five or more of the 11 effectiveness outcomes

b) After the discussion of a follow-up report: the Plenary could decide to place the member on enhanced follow-up at any stage in the regular follow-up process, if a significant number of priority actions have not been adequately addressed on a timely basis.

111. **Enhanced Follow-up (Expedited)**: Members with very serious deficiencies may be placed under the category of enhanced follow-up (expedited):

a) After the discussion of the MER: a member will be placed immediately on enhanced follow-up (expedited) if it has 10 or more of the following 13 Recommendations rated NC/PC for technical compliance: R.3, 5, 10, 11, 20 (core); and R.1. R.4, R.6, R.26, R.29, R.36, R.37, R.40; or

b) It has a low or moderate level of effectiveness for nine or more of the 11 effectiveness outcomes.

c) After the discussion of a follow-up report: the Plenary could decide to place the member on enhanced follow-up (expedited) at any stage in the follow-up process, if a significant number of priority actions have not been adequately addressed on a timely basis (for members already subject to enhanced follow-up) or in exceptional circumstances such as a significant decline in technical compliance or effectiveness (for members on regular follow-up).

112. **Annual Reporting**: Members on enhanced follow-up will provide a short (1 – 2 page) summary of progress against the recommendations contained in their MER one year after adoption of the MER, as part of their annual Status Report. Members on enhanced follow-up will provide their first detailed follow-up report on an annual basis beginning two years after adoption of the MER. The member should send the detailed progress report to the Secretariat setting out the actions it has taken since its MER, or is taking to address the priority actions and recommendations, and deficiencies outlined in its MER. This should include relevant changes to laws, regulations, guidance etc., as well as relevant data and information relating to effectiveness, and other contextual and institutional information. The expectation is that satisfactory progress should be reported in each detailed progress report, failing which the member could be moved to expedited reporting.

113. **Expedited Reporting**: For members placed on enhanced follow-up (expedited) on adoption of the member's MER, or at any other time, the Plenary will decide on the frequency and time of the member's follow-up reporting. The Plenary may impose quarterly reporting, and in the most serious cases, monthly reporting requirements, until such time the issues have been satisfactorily addressed.

114. **Secretariat/Team analysis:** For members under enhanced follow-up, the Secretariat will undertake the analysis of the member's report and prepare an analysis report, unless there is re-rating for technical compliance [to Largely Compliant or Compliant] and/or the use of an APG review team is warranted by other circumstances, in which case a review team comprised of experts from APG

members and observers (drawing on former assessment team members whenever possible) will undertake the analysis.

115. **Analysis Report:** Irrespective of whether a review team or the Secretariat undertakes the analysis, this is a desk-based review, however to the extent possible issues relating to effectiveness will also be considered. *Examples* of substantive issues include:

- Significant progress in the member leading to an increase in technical compliance or effectiveness.
- Significant changes in the member leading to a decline in technical compliance or effectiveness.
- Insufficient progress made by the member against the priority actions in its MER.
- Sufficient or insufficient progress made against actions agreed by members in more serious cases.
- For members under enhanced follow-up (expedited), progress in technical compliance against any one or more of the 13 Recommendations rated NC/PC.
- The analysis report involves re-rating [to Largely Compliant or Compliant] for any one or more of the FATF 40 Recommendations (Review Team only).
- The analysis report recommends removing the member from enhanced follow-up or enhanced follow-up (expedited).

116. **MEWG and APG Steering Group**: All analysis reports, including progress reports or expedited progress reports, for members under enhanced follow-up or enhanced follow-up (expedited), will be submitted to the MEWG for consideration and endorsement in the first instance. Thereafter, progress reports would either be (a) sent directly to members for adoption in the Annual Meeting; or (b) where the deficiencies identified are serious enough to warrant consideration of any measures under Graduated Steps (refer paragraph 118 below), progress reports would instead be sent to the APG Steering Group for consideration, before being circulated to members for adoption at the Annual Meeting or out-of-session, where appropriate.

117. **Plenary**: The Plenary will consider the analysis report and progress report and decide on the category of follow-up e.g. enhanced follow-up (expedited), including frequency and timing of reports; enhanced follow-up; or regular follow-up. Where expedited reports are involved (or under exceptional circumstances), this could be done out-of-session and not at the Annual Meeting.

118. **Graduated Steps**: In addition to more frequent reporting, the membership may also apply other enhanced measures to members placed on enhanced follow–up, as follows:

i. Send a letter from the APG Co-Chairs to the relevant Minister(s) drawing their attention to the evaluated member's lack of implementation/progress against the FATF standards and/or with APG ME follow-up requirements and/or membership requirements.
ii. Arrange a high level visit. This visit would meet with Ministers and senior officials.
iii. Refer the matter to the FATF for possible consideration under the FATF's ICRG process.
iv. In the context of the application of Recommendation 19 (former Recommendation 21) by members, issuing a formal APG statement to the effect that the member is insufficiently in compliance with the FATF Recommendations, and recommending appropriate action, and considering whether additional counter-measures are required.
v. Suspend a member from some/all APG activities until membership requirements are met.
vi. Terminate APG membership.

119. Step (i) above will apply to all members placed on enhanced follow-up. Subsequent steps may be applied to members on enhanced follow-up (expedited), as determined by the membership.

(c) MER Follow-up Assessment (on-site)

120. Whether under regular or enhanced follow-up, all assessed members will also have a follow-up assessment. This will normally take place five years after the adoption of the member's MER.

121. The follow-up assessment is intended to provide a more comprehensive update on the member's AML/CFT regime and to serve a similar function as an update that is part of a member's Financial Sector Assessment Programme. The focus is on the progress made by the member on the priority actions in its MER and other areas where the member had significant deficiencies. The follow-up assessment could also examine any areas where the Standards had changed since the MER, other elements of the member's AML/CFT regime which had changed significantly, as well as high risk areas identified in the MER or noted subsequently during the follow-up process.

122. The process for the follow-up assessment should include a short (two to three days) on-site visit to assess improvements in effectiveness and other areas. This on-site visit is to be conducted by a small team of (*e.g.* one to three) experts drawn from members or observers (preferably experts that were on the original assessment team) and supported by the Secretariat. The team will prepare a progress assessment report for Plenary discussion and decision. Re-ratings on both technical compliance and effectiveness are possible and the Plenary will decide whether the member should then be placed on regular or enhanced follow up, including applicable reporting time frames and other measures.

(d) Publication of Follow-Up Reports

123. The APG publication policy applies to actions taken under the APG's follow-up policy. Regular follow-up reports, and the follow-up assessment report (five years after the MER) will be published. The Plenary will retain flexibility on the frequency with which enhanced follow-up reports are published, but at a minimum reports will be published whenever there is a re-rating.

124. If requested by a member, a link will be provided from the APG website to a website of the member on which it has placed additional updates or other information relevant to the actions it has taken to enhance its AML/CFT system.

(e) *Follow-up for joint APG/FATF Members and other joint evaluations*

125. The follow-up process will differ for APG members subject to FATF follow-up processes. For the APG's joint APG/FATF members, the APG will rely primarily on the FATF's follow-up process. This will avoid duplication between the two bodies. For FATF members placed under regular follow-up, the first report to the APG will be the first available report provided to the FATF, which will be 2 ½ years after the FATF's adoption of the MER. Joint APG/FATF members' ME progress reports and any associated FATF Secretariat analysis will be distributed to all APG members and tabled at the APG Annual Meeting. For members of the APG who are also members of another FSRB or the GIFCS, but not members of the FATF, the APG follow-up procedures as described above (Section IX. Follow-up process) will apply, in consultation with the other assessing body.

X. Ex-Post review of major quality and consistency problems

126. Where an FATF member, the FATF Secretariat, or another assessment body considers that a draft APG MER has significant problems of quality or consistency, it should wherever possible raise such concerns with the APG prior to adoption. All draft MERs will be circulated to all assessment bodies,

as outlined above. The APG and FATF Secretariats should be notified of any such concerns in the first instance. The APG (assessment team and assessed member) should consider the concerns and work together to appropriately address them prior to the report being finalised.

127. There may however be highly exceptional situations where significant concerns about the quality and consistency of a MER remain after it has been adopted.

128. In order to ensure that the "FATF brand"[13] is not damaged by poor quality assessments, there will an ex-post review process, applying to all assessment bodies. The process will be based on the following:

a) The ex-post review should be applied only when serious or major issues of quality and consistency are identified, with the potential to affect the credibility of the FATF brand as a whole (e.g. where ratings are clearly inappropriate, are not consistent with the analysis, where there has been a serious misinterpretation of the Standards or the Methodology, or where an important part of the Methodology has been systematically misapplied).

b) Where there are significant concerns about the quality and consistency of an MER after its adoption, the APG and the FATF Secretariat should be informed in writing about those concerns within two weeks of the distribution of the MER following adoption. For such concerns to be considered further in this process, any specific concern should be raised by at least two of any of the following: FATF or FSRB members (not including the assessed member) or secretariats, or IFIs; at least one of which should have taken part in the adoption of the MER.

c) Any MER about which significant concerns have been raised will be circulated for consideration by the FATF Evaluation and Compliance Group (ECG), with a short note prepared by the FATF Secretariat (in consultation with APG), which also sets out the views of the assessment team and the assessed member.

d) The APG will not publish the MER until the issue is resolved within FATF and the APG.

e) The ECG will decide whether the report has significant problems of quality and consistency with the potential to affect the credibility of the FATF brand as a whole. In such cases ECG would make recommendations to the FATF Plenary on the appropriate action that could be taken (e.g. requesting that the APG reconsiders the report and/or makes appropriate changes before any publication). If the APG declines to respond to the action requested by the FATF, then the FATF Plenary will consider what further action may be necessary.

[13] This term is taken from the document *High Level Principles and Objectives of FATF and FATF Style Regional Bodies (FSRBs*), October 2012, which sets out the reciprocal rights and obligations of the FATF and FSRBs. On page 2 of the document it states that "Since the FATF and FSRBs are part of larger whole and the success or failure of one organisation can have an effect on all organisations, protection of the FATF brand is therefore in the common interest of both the FATF and FSRBs. The FATF brand is not limited to FATF output, but also extends to any FSRB output based on the FATF Recommendations, assessment methodology, best practice and guidance papers, mutual evaluations and follow-up." [emphasis added]. "FATF brand" issues are also discussed in more detail in Part C of the *High Level Principles* document.

APPENDIX 1 – TIMELINES FOR THE THIRD ROUND MUTUAL EVALUATION PROCESS

Date	Week	Key Indicative Milestones[14]		
		for Assessment Team	*for the Member*[15]	*for Reviewers*
At least six (6) months before the on-site	-24	• Commence research and desk-based review on technical compliance (TC). • Confirm (or find) assessors drawn from members which had volunteered[16]. Secretariat to formally advise member of the assessors once confirmed. • Invite delegations to provide information about (a) assessed member's risk situation and any specific issues which should be given additional attention by assessors, (b) their international cooperation experiences with the assessed member.	• Designate contact point(s) or person(s) and set up an internal coordination mechanisms (as necessary)[17]. • Respond to technical compliance (TC) update by completing TC questionnaire and providing updated information on new laws and regulations, guidance, institutional framework, risk and context.	
Four (4) months before the on-site	-16	• Prepare preliminary draft TC annex. • Analyse member's assessment of risk and discuss potential areas of increased focus for on-site[18]. • Confirm reviewers (drawn from pool of experts).	• Provide response on effectiveness based on the 11 Immediate Outcomes and the underlying Core Issues (including as relevant supporting information and data).	

[14] Interaction between assessors, Secretariat and member is a dynamic and continuous process. The assessment team should engage the assessed member as soon and as much as reasonably possible, and seeking and provision of information will occur throughout the process. Members should respond to queries raised by assessment team in a timely manner.

[15] The member would have to commence preparation and review of its AML/CFT regime for compliance with the FATF Standards more than 6 months prior to the on-site.

[16] The assessment team should comprise at least four assessors, including at least one legal, law enforcement and financial expert. Depending on the member and risks, additional assessors with the relevant expertise may be sought.

[17] Contact person(s) should ideally be familiar or trained in the FATF Standards before the commencement of the process.

[18] This may identify a need to request additional experts with other specific expertise for the assessment team.

Date	Week	Key Indicative Milestones[14]		
		for Assessment Team	*for the Member*[15]	*for Reviewers*
Three (3) months before the on-site visit	-12	• Send 1st Draft of TC annex (need not contain ratings or recommendations) to member for comments. • Members and FSRBs to provide specific information on their international co-operation experiences with the member. •	• Contact point(s) or person(s) to engage Secretariat to prepare for the on-site.	
Two (2) months before the on-site visit	-8	• Advise and consult member on preliminary areas of increased focus for on-site. This could involve preliminary discussions on the assessment team's impressions on the member's ML/TF risks. • Send draft scoping note to reviewers. • Prepare a preliminary analysis identifying key issues on effectiveness.	• Provide comments on draft TC assessment. • Commence work on draft programme for on-site visit	• Review draft scoping note
One (1) month before the on-site visit			Provide draft programme for on-site visit to the assessment team[19].	
At least three (3) weeks before the on-site	-3	• Finalise areas of increased focus for on-site visit, and key government agencies and private sector bodies to meet.		
At least two (2) week before the on-site	-2	• Finalise programme and logistics arrangements for on-site.		
		• Assessment team to prepare revised draft TC annex, draft TC text for MER, and outline of initial findings/key issues to discuss on effectiveness. Where possible a working draft MER prepared. Revised draft TC annex sent to member.	• Member to provide responses to any outstanding questions from the assessment team.	
On-site visit				

[19] Contact point(s) or person(s) to identify and inform government agencies and private sector bodies that will be involved in the on-site.

Date	Week	Key Indicative Milestones[14]		
		for Assessment Team	*for the Member*[15]	*for Reviewers*
Usually two (2) weeks (but may vary)	0	• Conduct opening and closing meetings with member. A written summary of key findings is to be provided at the closing meeting. • Where relevant, assessment team to review the identified areas for greater focus for the on-site. • Discuss and draft MER.		
After the on-site visit				
Within six (6) weeks of on-site visit	6	• Assessment team to prepare the complete 1st draft MER, and send to member for comments.		
Within four (4) weeks of receipt of draft MER	10	• Review and provide inputs on queries that member may raise.	*I.* Respond to 1st draft MER.	
Within two (2) weeks of receiving member comments	12	• Review member's response on 1st draft of MER. Prepare and send 2nd draft MER & ES to member (for information only) and reviewers. Send member comments to reviewers.		
	14			• Provide comments on 2nd draft MER, & ES.
Minimum – ten (10) weeks before the Plenary	15+	• Prepare and send 3rd draft MER & ES to member. • Send note to reviewers and assessed member setting out comments of assessment team on reviewers comments.		
Minimum – eight (8) weeks before the Plenary	17+	• If there are significant disagreements over technical compliance or effectiveness issues,	• Provide 2nd set of comments to the assessment team	

Date	Week	Key Indicative Milestones[14]		
		for Assessment Team	*for the Member*[15]	*for Reviewers*
		as identified either by the assessed member or assessment team, a face-to-face should be ideally held at least 8 weeks before the Annual Meeting (via video and tele-conference if needed).	• If needed, meet with the team to discuss any significant disagreements over the MER (via video and tele-conference if needed).	
Minimum - five (5) weeks before Plenary	18+	• Engage member and assessors on priority issues, and other comments received on MER or ES. • Circulate (a) compilation of delegation comments, and (b) finalised list of priority issues to be discussed in Plenary. • Send final draft MER & ES, together with reviewers' comments and assessment team response to all delegations for comments.	• Work with assessment team on priority issues, and other comments received on MER or ES	
Plenary Week	25+	**Pre –Plenary Discussions (if needed)** • Meet with the assessed member to discuss the mechanics and process for adoption of the report, not substantive issues, and the draft MER will not be subject to further change before the Plenary discussion, unless in exceptional circumstances.	• Meet with the assessment team to discuss the mechanics and process for adoption of the report, not substantive issues, and the draft MER will not be subject to further change before the Plenary discussion, unless in exceptional circumstances.	
Plenary Week	25[20]+	**Discussion of MER*** • Members discuss and then adopt the MER and Executive Summary.		

[20] Normally 25 week but the time period may also be extended or adjusted and based on justified circumstances (and with the consent of the assessed member).

Date	Week	Key Indicative Milestones[14]		
		for Assessment Team	*for the Member*[15]	*for Reviewers*
Post Plenary – Publication and Finalisation of MER*				
The MER adopted by Plenary is to be published as soon as possible. Within one (1) week: - The assessment team reviews the MER to take into account additional comments raised in Plenary, checks again for typographical errors, and sends to member. Within two (2) weeks: - The member confirms that the report is accurate and/or advises of any consistency, typographical or similar errors in the MER. - The FATF, FSRBs, or IFIs advise the FATF Secretariat and the APG Secretariat, in writing, if they have serious concerns about the quality and consistency of the MER, and if so, to indicate their specific concerns. - The APG will not publish the MER, or ES until those issues are resolved. Within six (6) weeks**:** - Where there is no such review process then the reports should be published within six weeks of adoption.				

APPENDIX 2 – AUTHORITIES AND BUSINESSES TYPICALLY INVOLVED FOR ON-SITE VISIT

Ministries:

- Ministry of Finance.
- Ministry of Justice, including central authorities for international co-operation.
- Ministry of Interior.
- Ministry of Foreign Affairs.
- Ministry responsible for the law relating to legal persons, legal arrangements, and non-profit organisations.
- Other bodies or committees to co-ordinate AML/CFT action, including the assessment of the money laundering and terrorist financing risks at the national level.

Criminal justice and operational agencies:

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

Financial sector bodies:

- Ministries/agencies responsible for licensing, registering or otherwise authorising financial institutions.
- Supervisors of financial institutions, including the supervisors for banking and other credit institutions, insurance, and securities and investment.
- Supervisors or authorities responsible for monitoring and ensuring AML/CFT compliance by other types of financial institutions, in particular bureaux de change and money remittance businesses.
- Exchanges for securities, futures and other traded instruments.
- If relevant, Central Bank.
- The relevant financial sector associations, and a representative sample of financial institutions (including both senior executives and compliance officers, and where appropriate internal auditors).
- A representative sample of external auditors.

DNFBP and other matters:

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

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

APPENDIX 3(a) – QUESTIONNAIRE FOR TECHNICAL COMPLIANCE UPDATE

APG THIRD ROUND MUTUAL EVALUATIONS

[*NAME OF MEMBER*]

CONTENT

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

1.1: Countries[21] 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)"]

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

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.

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 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).

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

5.4 TF offences should not require that the funds: (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.

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

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

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

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

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

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

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 1737 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 1737 of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to

(b) freezing action taken pursuant to UNSCR 1737 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 the relevant Security Council resolution; (ii) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity designated pursuant to UNSCR 1737; and (iii) the relevant countries have submitted prior notification to the 1737 Sanctions Committee 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)

8.1 Countries should:

(a) review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism, including NPOs.

(b) undertake domestic reviews of their NPO sector, or have the capacity to obtain timely information on its activities, size and other relevant features, using all available sources of information, in order to identify the features and types of NPOs that are particularly at risk of being misused for TF or other forms of terrorist support by virtue of their activities or characteristics.

(c) periodically reassess their NPO sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities.

8.2 Countries should conduct outreach to the NPO sector concerning TF issues.

8.3 Countries should have clear policies to promote transparency, integrity, and public confidence in the administration and management of all NPOs.

8.4 Countries should apply the following standards to NPOs which account for (i) a significant portion of the financial resources under the control of the sector; and (ii) a substantial share of the sector's international activities. Such NPOs should be required to:

(a) maintain information on: (i) the purpose and objectives of their stated activities; and (ii) the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information should be publicly available either directly from the NPO or through appropriate authorities;

(b) issue annual financial statements that provide detailed breakdowns of income and expenditure;

(c) have controls in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of the NPO's stated activities;

(d) be licensed or registered ;

(e) follow a "know your beneficiaries and associated NPOs" rule; and

(f) maintain, for a period of at least five years, records of domestic and international transactions , and the information in (a) and (b) above, and make these available to competent authorities upon appropriate authority.

8.5 Competent authorities should monitor the compliance of NPOs with Criterion 8.4, and should be able to apply proportionate and dissuasive sanctions for violations of the requirements by NPOs or persons acting on behalf of these NPOs.

8.6 Authorities should be able to investigate and gather information on NPOs, including through:

(a) domestic cooperation, coordination and information-sharing among authorities or organisations that hold relevant information on NPOs;

(b) full access to information on the administration and management of particular NPOs (including financial and programmatic information); and

(c) mechanisms to ensure that relevant information is promptly shared with competent authorities, in order to take preventive or investigative action, when there is suspicion or reasonable grounds to suspect that a particular NPO is: a front for fundraising by a terrorist organisation; or being exploited as a conduit for TF, including for the purpose of escaping asset freezing measures; or concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations.

8.7 Countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of TF or 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 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 a suspicious transaction report.

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

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.

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; and

(c) adequate safeguards on the confidentiality and use of information exchanged.

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 a suspicious transaction report or related information is being filed with the FIU.

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 (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or

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

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

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.

40.19 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 3 (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 is

clear 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

1.1. How well does the country understand its ML/TF risks?

1.2. How well are the identified ML/TF risks addressed by national AML/CFT policies and activities?

1.3. To what extent are the results of the assessment(s) of risks properly used to justify exemptions and support the application of enhanced measures for higher risk scenarios, or simplified measures for lower risk scenarios?

1.4. To what extent are the objectives and activities of the competent authorities and SRBs consistent with the evolving national AML/CFT policies and with the ML/TF risks identified?

1.5. To what extent do the competent authorities and SRBs co-operate and co-ordinate the development and implementation of policies and activities to combat ML/TF and, where appropriate, the financing of proliferation of weapons of mass destruction?

1.6. 1.6. To what extent does the country ensure that respective financial institutions, DNFBPs and other sectors affected by the application of the FATF Standards are aware of the relevant results of the national ML/TF 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

2.1 To what extent has the country provided constructive and timely mutual legal assistance and extradition across the range of international co-operation requests? What is the quality of such assistance provided?

2.2 To what extent has the country sought legal assistance for international co-operation in an appropriate and timely manner to pursue domestic ML, associated predicate offences and TF cases which have transnational elements?

2.3 To what extent do the different competent authorities seek other forms of international cooperation to exchange financial intelligence and supervisory, law enforcement or other information in an appropriate and timely manner with their foreign counterparts for AML/CFT purposes?

2.4 To what extent do the different competent authorities provide (including spontaneously) other forms of international co-operation to exchange financial intelligence and supervisory, law enforcement or other information in a constructive and timely manner with their foreign counterparts for AML/CFT purposes?

2.5 How well are the competent authorities providing and responding to foreign requests for 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 and DNFBPs for compliance with AML/CFT requirements commensurate with their risks.

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

3.1 How well does licensing, registration or other controls implemented by supervisors or other authorities prevent criminals and their associates from holding, or being the beneficial owner of a significant or controlling interest or holding a management function in financial institutions or DNFBPs? How well are breaches of such licensing or registration requirements detected?

3.2 How well do the supervisors identify and maintain an understanding of the ML/TF risks in the financial and other sectors as a whole, between different sectors and types of institution, and of individual institutions?

3.3 With a view to mitigating the risks, how well do supervisors, on a risk-sensitive basis, supervise or monitor the extent to which financial institutions and DNFBPs are complying with their AML/CFT requirements?

3.4 To what extent are remedial actions and/or effective, proportionate and dissuasive sanctions applied in practice?

3.5 To what extent are supervisors able to demonstrate that their actions have an effect on compliance by financial institutions and DNFBPs?

3.6 How well do the supervisors promote a clear understanding by financial institutions and DNFBPs of their AML/CFT obligations and ML/TF risks?

Immediate Outcome 4: Financial institutions and DNFBPs 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

4.1 How well do financial institutions and DNFBPs understand their ML/TF risks and AML/CFT obligations?

4.2 How well do financial institutions and DNFBPs apply mitigating measures commensurate with their risks?

4.3 How well do financial institutions and DNFBPs apply the CDD and record-keeping measures (including beneficial ownership information and ongoing monitoring)? To what extent is business refused when CDD is incomplete?

4.4 How well do financial institutions and DNFBPs 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?

4.5 To what extent do financial institutions and DNFBPs meet their reporting obligations on the suspected proceeds of crime and funds in support of terrorism? What are the practical measures to prevent tipping-off?

4.6 How well do financial institutions and DNFBPs 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

5.1 To what extent is the information on the creation and types of legal persons and arrangements in the country available publicly?

5.2 How well do the relevant competent authorities identify, assess and understand the vulnerabilities and the extent to which legal persons created in the country can be, or are being misused for ML/TF?

5.3 How well has the country implemented measures to prevent the misuse of legal persons and arrangements for ML/TF purposes?

5.4 To what extent can relevant competent authorities obtain adequate, accurate and current basic and beneficial ownership information on all types of legal persons created in the country, in a timely manner?

5.5 To what extent can relevant competent authorities obtain adequate, accurate and current beneficial ownership information on legal arrangements, in a timely manner?

5.6 To what extent are effective, proportionate and dissuasive sanctions applied against persons who do not comply with the information requirements?

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

6.1 To what extent are financial intelligence and other relevant information accessed and used in investigations to develop evidence and trace criminal proceeds related to ML, associated predicate offences and TF?

6.2 To what extent are the competent authorities receiving or requesting reports (e.g., STRs, reports on currency and bearer negotiable instruments) that contain relevant and accurate information that assists them to perform their duties?

6.3 To what extent is FIU analysis and dissemination supporting the operational needs of competent authorities?

6.4 To what extent do the FIU and other competent authorities co-operate and exchange information and financial intelligence? How securely do the FIU and competent authorities protect the confidentiality of the information they exchange or use?

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

7.1 How well, and in what circumstances are potential cases of ML identified and investigated (including through parallel financial investigations)?

7.2 To what extent are the types of ML activity being investigated and prosecuted consistent with the country's threats and risk profile and national AML/CFT policies?

7.3 To what extent are different types of ML cases prosecuted (e.g., foreign predicate offence, third-party laundering, stand-alone offence etc.) and offenders convicted?

7.4 To what extent are the sanctions applied against natural or legal persons convicted of ML offences effective, proportionate and dissuasive?

7.5 To what extent do countries apply other criminal justice measures in cases where a ML investigation has been pursued but where it is not possible, for justifiable reasons, to secure a ML conviction? Such alternative measures should not diminish the importance of, or be a substitute for, prosecutions and convictions for ML offences.

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

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

8.1 To what extent is confiscation of criminal proceeds, instrumentalities and property of equivalent value pursued as a policy objective?

8.2 How well are the competent authorities confiscating (including repatriation, sharing and restitution) the proceeds and instrumentalities of crime, and property of an equivalent value, involving domestic and foreign predicate offences and proceeds which have been moved to other countries?

8.3 To what extent is confiscation regarding falsely / not declared or disclosed cross-border movements of currency and bearer negotiable instruments being addressed and applied as an effective, proportionate and dissuasive sanction by border/custom or other relevant authorities?

8.4 How well do the confiscation results reflect the assessments(s) of ML/TF risks and national AML/CFT policies and priorities?

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

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

9.1. To what extent are the different types of TF activity (e.g., collection, movement and use of funds) prosecuted and offenders convicted? Is this consistent with the country's TF risk profile?

9.2. How well are cases of TF identified, and investigated? To what extent do the investigations identify the specific role played by the terrorist financier?

9.3. To what extent is the investigation of TF integrated with, and used to support, national counter-terrorism strategies and investigations (e.g., identification and designation of terrorists, terrorist organisations and terrorist support networks)?

9.4. To what extent are the sanctions or measures applied against natural and legal persons convicted of TF offences effective, proportionate and dissuasive?

9.5. To what extent is the objective of the outcome achieved by employing other criminal justice, regulatory or other measures to disrupt TF activities where it is not practicable to secure a TF conviction?

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

10.1. How well is the country implementing targeted financial sanctions pursuant to (i) UNSCR1267 and its successor resolutions, and (ii) UNSCR1373 (at the supra-national or national level, whether on the country's own motion or after examination, to give effect to the request of another country)?

10.2. To what extent, without disrupting legitimate NPO activities, has the country implemented a targeted approach, conducted outreach, and exercised oversight in dealing with NPOs that are at risk from the threat of terrorist abuse?

10.3. To what extent are terrorists, terrorist organisations and terrorist financiers deprived (whether through criminal, civil or administrative processes) of assets and instrumentalities related to TF activities?

10.4. To what extent are the above measures consistent with the overall TF risk profile?

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

11.1. How well is the country implementing, without delay, targeted financial sanctions concerning the UNSCRs relating to the combating of financing of proliferation?

11.2. To what extent are the funds or other assets of designated persons and entities (and those acting on their behalf or at their direction) identified and such persons and entities prevented from operating or executing financial transactions related to proliferation?

11.3. To what extent do financial institutions and DNFBPs comply with, and understand their obligations regarding targeted financial sanctions relating to financing of proliferation?

11.4. How well are relevant competent authorities monitoring and ensuring compliance by financial institutions and DNFBPs with their obligations regarding targeted financial sanctions relating to financing of proliferation?