Financial Action Task Force
Groupe d'Action Financière

30-Apr-2013

English - Or. English

FATF/PLEN/M(2013)1
For Official Use

Plenary

SUMMARY RECORD OF THE SECOND PLENARY OF FATF-XXIV (FEBRUARY 2013) - Non-Confidential Items

20-22 February 2013, OECD Conference Centre, Paris, France

FATF-XXIV

Rick MCDONELL, Tel.: +(33-1) 45 24 16 08, rick.mcdonell@fatf-gafi.org

JT03338940

English - Or. English

SUMMARY RECORD OF THE SECOND PLENARY OF FATF-XXIV (FEBRUARY 2013)

NON-CONFIDENTIAL ITEMS

20-22 February 2013, OECD Conference Centre, Paris, France

The meeting was chaired by Bjørn S. Aamo (FATF President).

For the confidential items, please see FATF/PLEN/M(2013)2.

DAY 1: WEDNESDAY, 20 FEBRUARY 2013, 14h00 – 18h00

A. INTRODUCTION	Document references
1. Introductory remarks from the President (commenting on some of the agenda items):	Oral report

- A new item is the important topical issue concerning the implementation of our standards by global financial players and the challenges for both industry and authorities in this connection. We look forward to the presentation by our US and UK colleagues.

- The completion of the Methodology which will guide assessors in conducting the 4th round of evaluations is the most important item on our agenda. Delegations, the Working Groups, the Co-chairs and the Secretariat have all put a lot of hard work into this process. I hope the Plenary will be able to discuss and conclude any remaining issues.

- How we should proceed with a possible and the expansion of the FATF-membership is another important item. We will need to consider carefully how we are to proceed on this. The creation of an *ad hoc* group is an important step in the right direction. We should note that the interest in becoming part of the FATF is definitely there. In addition to the two formal applications received last summer, from Israel and Lebanon, we have received applications from the United Arab Emirates and from Ukraine.

- We plan to discuss at this Plenary how we might improve our organisational and working methods. Although there is general agreement that FATF broadly speaking has an effective and flexible internal organisation, it is important from time to time to review our working methods and improve them wherever possible.

- The development of the global network of the FATF and the FSRBs is an important part of the objectives of the President for this year. The GNCG is working systematically on how the FSRBs might learn from each other when it comes to working methods and organisation. I have had the pleasure of taking part in the Plenary meetings of five of the FSRBs so far, and the Vice President has participated in one. The meetings showed a strong spirit and responsibility in taking on the obligations as partners in the global fight against money laundering and terrorist financing.

- FATF has continued its close co-operation with the IMF and the World Bank, not least on developing the Methodology that all assessment bodies will be using in their evaluations. Our

close co-operation with the United Nations was marked by participation of the Executive Secretary and myself in a high-level meeting in November concerning co-operation between the UN and the FATF on implementation of anti-terrorism measures. The Public Statement by the President of the UN Security Council issued on 15 January showed strong support for the work of the FATF.

- The FATF is engaged in a broad communication and dialogue with the private sector. We are planning for a meeting of the Consultative Forum in late April in London, where the new Methodology will be a major item. Back to back with this meeting we intend to have a special dialogue meeting with representatives of the NPOs to discuss issues related to Recommendation 8.

- As part of a better and more direct dialogue with major financial institutions, there will be a meeting between FATF representatives and members of the Wolfsberg Group in Paris in late March.

- We look forward to reports from the Working Groups. It seems that we may provide good news to the world: Several countries have made progress, they have addressed deficiencies and brought legislation and regulation better in line with the FATF recommendations.

B. FOLLOW-UP TO MUTUAL EVALUATIONS

2. Follow-up to Mutual Evaluations of Members in the Context of Membership Action Plans

a)	India – 7th Follow-up Report / Progress Report on Action Plan	FATF/PLEN(2013)1

Decisions taken:

- India's 7th follow-up/progress report was adopted.

- The Plenary decided to consider India's eighth follow-up report with a view to India's removal from the regular follow-up process at the June 2013 plenary meeting.

Important issues raised:

- Amendments to India's AML/CFT legislation recently came into force. They ensure strong technical compliance mainly with regard to R.1, R.3 and SR.II. In addition, India has taken the necessary steps to address the outstanding deficiencies with regard to beneficial ownership requirements and has now addressed all of the R.5 technical shortcomings identified in the 2010 MER. These recent actions substantially complete India's *Action Plan to strengthen India's AML/CFT System.*

- The Plenary noted that since the adoption of its MER in June 2010, India has made remarkable progress with regard to the implementation of its action plan, including with respect to the nine core and key Recommendations that were rated PC.

- India reiterated its commitment to the implementation of an effective AML/CFT regime at the highest political level as well as at bureaucratic and operational levels. India also provided an update on on-going implementation and pointed to improvement of its effectiveness in relation to R.1, R.3 and SR.II.

- The Russian Federation; Hong Kong, China; the US; Brazil; APG; EAG; Germany; Canada; Korea; China; Japan; the UK; Turkey; Argentina and Australia congratulated India on the significant progress made since the adoption of its MER and corresponding action plan in June 2010 and supported the FATF Secretariat's proposal to draft a detailed follow-up report with a view to removing India from the FATF's regular follow-up process for discussion in June 2013.

- The US, Canada and Australia proposed that given the workload involved in drafting and discussing detailed follow-up reports, the FATF Secretariat draft a summary report for discussion by the June 2013 Plenary.

- The FATF Secretariat clarified that the third round mutual evaluation follow-up procedures require that in support of the discussion, a detailed report with a clear overview and assessment of measures taken to address the deficiencies identified in the MER needs to be made available to FATF delegations. A summary of that report could be delivered to the next Plenary.

3. Follow-up to Mutual Evaluations of Members under the Enhanced Process

a) Argentina – 7th Follow-up Report — FATF/PLEN(2013)4

Decisions taken:

- Due to the number and scope of the deficiencies that remain, Argentina will remain in the enhanced follow-up process and report back to the June 2013 Plenary.

Important issues raised:

- The Plenary noted the comments from the US on the new structure in the prosecutor's office as a step in the right direction to facilitate a more effective prosecution of ML/FT cases. Argentina will need time to implement this new structure to ensure that it works.

- The Plenary also heard Argentina's response to a question from Canada, indicating that the aim of the change in the public prosecutor's office is to create a much larger AML/CFT unit and strengthen and improve the AML/CFT system.

b) Australia – 10th Follow-up Report — FATF/PLEN(2013)5

Decisions taken:

- Australia remains under the enhanced follow-up process and will report back to the next FATF Plenary meeting in June 2013.

- To send a letter to the new Attorney General expressing concern about the lengthy delays in issuing the consultation document and in rectifying the deficiencies under R.5, as well as indicating the possibility of a high level visit if satisfactory progress is not made.

- To give the President the authority to arrange a high level mission to Australia if required and with the flexibility to determine the dates.

Important issues raised:

- Canada and the US noted that there are some important deficiencies and that progress needs to be made soon, and that it is important that there is political support for the changes.

- The Netherlands, the UK, France, Germany, Norway, and Switzerland noted the lack of progress, expressed concern about the long delays and agreed with the proposal of the President that a letter be sent first, and that if the required progress is not made with a reasonable time then there should be a high level mission.

- APG offered to join any high level mission that may eventuate.

c) Japan – 5th Follow-up Report	FATF/PLEN(2013)6

Decisions taken:

- The fifth follow-up report of Japan was adopted.

- Japan remains under enhanced follow-up process and will report back to the FATF at the next Plenary meeting in June 2013.

- The Plenary also decided that a high-level mission to Japan should be arranged in order to convey the FATF's concerns to the relevant Ministers; however, it agreed that the FATF should be flexible as to when the mission will take place in order to be as beneficial as possible for Japan and therefore it need not take place before the June Plenary but should take place before the October Plenary.

d) Turkey – 10th Follow-up Report	FATF/PLEN(2013)7

Decisions taken:

- On 7 February 2013, the Turkish Grand National Assembly adopted the Law on the Prevention of the Financing of Terrorism, which was signed into law on 15 February 2013. The FATF Plenary welcomed this action and recognised that the new legislation is an important step forward for Turkey in improving compliance with SR.II and SR.III.

- In spite of this positive step, there still remain a number of ongoing shortcomings in the Turkish counter-terrorist financing regime. Turkey will need to address these shortcomings, either through amendments to its legislation or through other legal and/or administrative instruments, in order to reach a satisfactory level of compliance with the FATF standards which is at a level equivalent to LC.

- Turkey has committed to addressing the remaining terrorist financing issues. To do so, Turkey will submit, prior to the next FATF meeting in June 2013, a report on how the remaining SR.II and SR.III shortcomings are being addressed.

- Given the progress made with the enactment of the Law on the Prevention of the Financing of Terrorism and Turkey's clear commitment to address remaining deficiencies, the FATF decided not to suspend Turkey.

- The Plenary also decided to include a statement on Turkey's situation in the public Chairman's Summary.

4. Other Follow-up Reports

a) Canada – 5th Follow-up Report — FATF/PLEN(2013)2

Decisions taken:

- The Plenary decided that Canada should report back in February 2014, after the amendments to the *Proceeds of Crime Money Laundering and Terrorist Financing* (PCMLTF) Regulations, adopted on 31 January 2013, have come into force.

- The Plenary also noted that given the progress that these regulatory amendments will bring in relation to R.5, Canada will be in a position to apply for removal from the follow-up process in February 2014.

Important issues raised:

- Canada informed the Plenary that, by February 2014, guidance will be developed by the Office of the Superintendent of Financial Institutions (OSFI) and the Canadian FIU (FINTRAC), to clarify some of the provisions of the new Regulations.

- The US, the Russian Federation, the APG, Germany, Australia and Mexico congratulated Canada on the progress made. The US and Australia underlined the importance of having a process in place to demonstrate the rationale for (low risk) exemptions.

b) United States – 10th Follow-up Report — FATF/PLEN(2013)16

Decisions taken:

- The US will report back in writing to the Plenary in June 2013, including text of the Proposed Rule.

Important issues raised:

- The US reported that five public hearings were held on the draft regulation—the Advanced Notice of Proposed Rule Making (ANPRM). The ANPRM includes all four elements of CDD, and defines beneficial ownership to include both ownership and control based on a threshold, but does not require verification of beneficial ownership status. A Proposed Rule is currently being drafted, and will be issued for public comment in a few weeks. Adoption of the Final Rule is possible by June 2013, but will more likely occur some months later, and will be followed by a waiting period to allow time for financial institutions to implement the new requirements (likely one year).

- The Plenary welcomed the progress reported. Canada noted the importance of sharing experience on these issues, particularly concerning group wide policies. APG highlighted the positive effect these new measures will have in the Asia Pacific region. The Russian Federation welcomed the opportunity to study the text of the Proposed Rule.

- France noted the importance of beneficial ownership, and suggested that the FATF have an informal discussion with other relevant international organisations to advance the subject further.

C.	**FATF MEMBERSHIP & REQUEST FOR FATF OBSERVER STATUS [CLOSED SESSION]**	
5.	Expansion of FATF Membership: Next Steps	FATF/PLEN(2013)8
6.	Composition of Ad Hoc Group on Membership	FATF/PLEN/RD(2013)2

[See FATF/PLEN/M(2013)2]

DAY 2: THURSDAY, 21 FEBRUARY 2013, 9h00 – 18h00		
C.	**FATF MEMBERSHIP & REQUEST FOR FATF OBSERVER STATUS [CLOSED SESSION]** ***[continued]***	
7.	Discussion of Other Membership Issues [if required]	FATF/PLEN/RD(2013)3
8.	Request from the Organisation for Security and Co-operation in Europe (OSCE) for status as an FATF observer	FATF/PLEN(2013)9

[See FATF/PLEN/M(2013)2]

D.	**FATF BUDGET [CLOSED SESSION]**	
9.	FATF Budget Update	FATF/PLEN(2013)10

[See FATF/PLEN/M(2013)2]

E.	**FORWARD PLANNING OF FATF WORK**	
10.	Forward Planning of FATF Work: Review of Organisational and Working Methods	FATF/PLEN(2013)11
11.	Consolidated FATF Work Plan (2013-2014)	FATF/PLEN(2013)12

Decisions taken:

- There was support for measures to revitalise the role of the Plenary and to consider measures to improve processes for setting priorities and longer term planning. Strategic elements that may be included in the Mid-term review of the Mandate in 2016 should be prepared.

- The Plenary agreed with the President to work on making the responsibilities of each of the working groups more precise – with the possibility of some changes in names – when the mandates of the groups are presented for adoption in June. The approach taken at this stage will be pragmatic; to clarify responsibilities and avoid unnecessary overlaps, changes will be proposed as needed. The President will co-operate with the Vice-President and the Secretariat in preparing for decisions in June.

- The President will submit a preliminary report to FATF Ministers on the latest FATF developments following this Plenary meeting.

- The Vice-President in his objectives for the next presidency will make an initial proposal on prioritisation of individual FATF and working group tasks (as indicated in the consolidated work plan) for consideration by the June Plenary meeting.

Important issues raised:

- The Plenary agreed with the President that now is the time to undertake strategic planning prior to the start of the next round of mutual evaluations. It also agreed that there is a need to further emphasise the primacy of the role of the Plenary vis-à-vis oversight, setting of priorities for the working groups and the FATF as a whole and the need for more substantive discussion of selected issues.

- In looking at the working group structure, there was broad agreement that the approach taken to any restructuring should be pragmatic and should focus on fixing things that are not working well rather than simply for the sake of change. There was general agreement that the ICRG function should be maintained and remain separate, and there was broad support for further focus on policy development separate from management of the evaluation process.

F. INFORMATION ON IMPLEMENTATION OF AML/CFT STANDARDS

12. *The AML/CFT Standards and Global Financial Players: Challenges for Industry and for Authorities*

The Plenary heard two presentations from the US and UK respectively, concerning challenges for industry and for authorities.

The presentations highlighted a number of deficiencies in how global financial groups were implementing the FATF Standards and the gaps between proper regulatory and supervisory oversight which a number of recent cases have identified. There was discussion about how these challenges might be met at the domestic level and also what role the FATF might consider taking in the future on issues that have global relevance to the implementation of the Standards. It was agreed that the FATF would further consider supervision and enforcement issues at future Plenaries.

G. MONITORING THE IMPLEMENTATION OF AML/CFT MEASURES

13. Report by the WGEI Co-chairs — FATF/PLEN/RD(2013)4

Decisions taken:

- The WGEI Co-Chairs report was adopted with minor amendments. The decisions endorsed included: (i) the adoption of the revised Guidance on AML/CFT measures and financial inclusion (see below); (ii) agreement for Mexico to report back to Plenary in June on its progress; and (iii) holding the next meeting of the private sector consultative forum in London in April 2013.

Important issues raised:

- *4th Round Process and Procedures*: Canada and the MENAFATF requested further clarifications on the 4th round process and procedures and it was noted that in the lead up to June 2013, delegations would have an opportunity to provide written comments. The US and France reiterated that the 4th round process and procedures, including the contents of the MER template, should be viewed as a package, taking into account the overall resource implications.

- The World Bank and IMF noted that the 5-year FSAP cycle for systemically important countries is mandatory although further consideration should be given to improving the linkages between the FSAPs and AML/CFT assessment processes and schedules.

- *4th Round Assessor Training*: There was strong interest from Canada and CFATF in the conduct of training for the 4th round. The World Bank indicated its interest in working with the FATF and other assessment bodies to develop training materials, and the UN indicated its willingness to contribute to developing the training materials relating to financing of proliferation and terrorist financing.

- *Follow-Up Reporting*: Canada requested that the Plenary be updated on the progress of 3rd round follow-up by members. The Co-Chairs agreed that this is a regular part of WGEI's work and could be discussed in June 2013.

- The President noted that the Co-Chairs' report is a summary of the key points raised and will not be able to reflect every discussion point raised during the meeting.

14. FATF Methodology 2013 — FATF/WGEI(2013)1

Decisions taken:

- The *FATF Methodology 2013* was adopted with the resolution of the issues relating to: (i) a compromise set of descriptions for technical compliance ratings, (ii) revised text to include a reference to alternative measures to ML prosecutions in the context of effectiveness (IO.7) (i.e. adding a reference to "Such alternative measures should not diminish the importance of, or be a substitute for, prosecutions and convictions for ML offences" in *core issue* 7.5), and (iii) removing the reference to "identify and assess" in *core issue* 1.1.

Important issues raised:

- *Descriptions of technical compliance ratings*: Following the end of the WGEI meeting, interested delegations worked to develop a compromise to ensure continuity between the 3rd round and 4th round ratings, including the need to take into account the number and relative importance of the

criteria met or not met, while avoiding an inconsistency between the descriptions in the ratings box. The compromise was adopted in Plenary without objection.

- *Alternative measures to ML prosecutions in IO.7*: The issues discussed by Plenary were: (a) whether this is a principle to which the FATF should subscribe, and (b) if so, whether it should be included as a *core issue*, or alternatively as a *specific factor*.

- While noting the majority support for recognising such alternative measures, the Netherlands, the US, South Africa and Hong Kong, China reiterated their concerns that its inclusion may send a wrong message to external parties and detract from the FATF's focus on encouraging countries to pursue ML prosecutions and convictions. Other delegations supporting its inclusion reiterated that inclusion of such alternative measures in IO.7 is meant to be limited in scope and not intended to detract from the FATF's focus on money laundering. It allows credit to be given to countries in cases where efforts have been expended to pursue the money laundering cases, but where, due to justifiable reasons, the ML prosecutions or convictions could not be pursued, and offenders are prosecuted for other criminal offences.

- It was clarified that the context for alternative measures in *core issue* 7.5 and *core issue* 9.5 are different, and in the context of terrorist financing, alternative measures are adopted to prevent or disrupt a terrorist act from occurring.

- *Removing "identify and assess" in core issue 1.1*: Canada noted that the assessment of effectiveness should focus on a country's understanding of its ML/TF risks, and the steps taken to mitigate it. Issues relating to the identification and assessment of the ML/TF risks would be dealt with in the technical compliance assessment. The US, the Netherlands, the UK, Australia, Luxembourg, Germany and Sweden also supported deleting the references in *core issue* 1.1. The Netherlands further noted that the assessment of effectiveness will be a learning process for the first few evaluations.

15. 4th Round Assessments – Plenary Discussion — FATF/PLEN/RD(2013)5

Decisions taken:

- The Plenary agreed to include the reference to DNFBPs in R.37 in the Standards (i.e. DNFBP secrecy/confidentiality should not affect the provision of mutual legal assistance). The corresponding change in the Methodology was also adopted. The change in the Standards would be reflected immediately in the electronic version of the Standards on the FATF website, and in the next revised print edition. This will also be indicated clearly by way of an Annex of substantial changes.

- In noting the potential overlaps with the ongoing work on data protection and privacy, it was also agreed that the review of R.9 should include consideration of the issue of whether R.9 should also include a possible reference that DNFBP secrecy / confidentiality laws should not inhibit the implementation of the FATF Recommendations.

Important issues raised:

- GAFISUD sought clarification that the changes to R.37 would not require the FSRBs to endorse the Standards again. The President responded by saying that we could implicitly accept that FSRBs

will use the authorised version of the Recommendations and the Methodology as they appear on the FATF website.

16.	Revised Guidance on AML/CFT measures and financial inclusion	FATF/WGEI(2013)4

Decisions taken:

- The revised Guidance on AML/CFT measures and financial inclusion was adopted.

Important issues raised:

- The World Bank, the US and the APG noted their support and the importance of this work. The APG and the World Bank also reiterated the need to ensure that the guidance is widely circulated.

H. PUBLIC DOCUMENT

17.	Draft Chairman's Summary	FATF/PLEN/RD(2013)6

Decisions taken:

- The Plenary agreed to publish the Chairman's Summary following the meeting subject to certain changes suggested by delegations. The ICRG statements would also be published as separate documents as has occurred after previous Plenary meetings.

Important issues raised:

- The statement on Turkey was discussed and agreed separately (see item 3d above).

DAY 3: FRIDAY, 22 FEBRUARY 2013, 9h00 – 18h00

I. INTERNATIONAL CO-OPERATION AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

18.	Report by the ICRG Co-chairs	FATF/PLEN/RD(2013)7

Decisions taken:

- The report of the ICRG Co-Chairs, including the Public Statement and compliance document, was adopted with minor changes. This includes the following decisions:

  -remove Ghana and Venezuela from ICRG review;

  -organise an onsite visit, through the Americas RRG, to Bolivia prior to the June 2013 plenary to confirm that the implementation of reforms has begun and is being sustained;

-organise an onsite visit, through the Asia/Pacific RRG, to Brunei Darussalam, the Philippines, Sri Lanka and Thailand, prior to the June 2013 plenary to confirm that the implementation of reforms has begun and is being sustained

- due to Turkey's significant progress in enacting CFT legislation, there was no need for countermeasures (reference was made to the follow-up report on Turkey discussed in item 3 d above)

-to conduct a targeted review of Lao PDR and a prima facie review of Iraq by the June 2013 ICRG meeting.

- The Plenary discussed the next procedural steps for dealing with Turkey which is subject to both the Plenary's enhanced mutual evaluation follow-up process and ICRG monitoring. To avoid duplication of efforts, it was agreed that the Europe/Eurasia RRG, during its next meeting, will discuss progress made through the new CFT legislation, including an analysis of this legislation, as well as how Turkey aims to address the remaining shortcomings. The FATF Secretariat will coordinate the procedural aspects and ensure that all delegations are notified of this meeting; any interested delegations would be strongly encouraged to participate. The results of this discussion would inform both the Europe/Eurasia RRG co-chair's report to the June 2013 ICRG meeting as well as the FATF Plenary's discussion of the progress made by Turkey in the follow-up process.

Important issues raised:

- The ICRG co-Chairs thanked delegations for their increased participation in the four RRGs which enhances the capacity of the Co-Chairs and the FATF Secretariat in managing the ICRG workload.

- Based on a proposal by MENAFATF, which was supported by France, the Plenary decided to improve the language with respect to Morocco in the separate section of the *compliance document* to underline that Morocco has only one remaining deficiency to address.

- The Plenary agreed with the proposal of GAFISUD to include both in the ICRG Co-Chairs's report and the compliance document that Cuba has recently become a member of GAFISUD.

- The APG reiterated its request for consolidated ICRG procedures; MENAFATF indicated that it had some discussions of the ICRG process at their plenary and that it had submitted written comments on the ICRG process which could also be taken into account.

- The ICRG Co-Chairs announced that they will work with the FATF Secretariat on a paper about the future direction of the ICRG consistent with the upcoming 4th round of mutual evaluations and will have an initial discussion at the June 2013 ICRG meeting.

J. TYPOLOGIES

19.	Report by the WGTYP Co-Chairs	FATF/PLEN/RD(2013)8

Decisions taken:

- The report of the WGTYP Co-Chairs was adopted (subject to editorial changes).

- The Plenary welcomed Mr. Martin TABI (Canada) as new WGTYP Co-chair.

Important issues raised:

- The APG reminded the Plenary about the joint APG/EAG Meeting of Experts on Typologies that will take place in Ulan Bator, Mongolia, in September 2013 and offered the venue as a possible location for the ICRG Asia Pacific regional review group meeting ahead of the October 2013 FATF Plenary.

- The FATF private sector consultation on the draft typologies report dealing with legal professions will take place in May 2013 in London. Canada raised the point that more effort should be undertaken to consolidate meetings (for example, this meeting with the FATF private sector consultation that will take place in April) to permit more efficient use of travel resources. The Secretariat indicated that the legal profession as a sector was somewhat different from the sectors involved in the April consultation. Furthermore, the timing of the consultation is being driven by the availability of the UK Law Society facility and the calendar for completion of the typologies report by June 2013.

- MENAFATF indicated that they hoped to be able to propose organising the annual meeting of experts on typologies jointly with FATF this year. If they are able to do it, then they will make the formal proposal in June.

20. Guidance on National Risk Assessment	FATF/WGTY/WD(2012)3/REV5

Decisions taken:

- The Plenary adopted the guidance, *National ML/TF Risk Assessment*, (with minor modifications – see annex to the Report of the WGTYP Co-Chairs). The document will be published on the FATF public website.

Important issues raised:

- The WGTYP Co-Chairs indicated that the WGTYP hoped to keep this guidance as a "living document" by periodically supplementing it with descriptions of national risk assessment initiatives as these become available.

21. "Mapping Exercise" on tax crimes (related to direct and indirect taxes) as a predicate offence for money laundering	FATF/WGTY(2012)36/REV1

Decisions taken:

- The Plenary adopted the report, *"Mapping Exercise" on tax crimes (related to direct and indirect taxes) as a predicate offence for money laundering,* (with minor modifications – as indicated in the Report of the WGTYP Co-Chairs). The document is not intended to be published on the FATF public website; however, it will be shared widely among national authorities and other interested international organisations to serve as a baseline of relevant information on FATF members.

Important issues raised:

- Greece indicated that more work could be undertaken in this area and urged the Plenary to decide quickly on future steps that could result from this work. Italy suggested that the FATF gather further information, particularly regarding practical cases that could serve as the basis for guidance. Switzerland, supported by the US; Hong Kong, China; and Luxembourg, noted that more information could be collected from countries on relevant cases and proposed that WGTYP seek presentations on country examples. Norway and Netherlands volunteered to present relevant cases during the June meeting in Oslo.

- The President proposed that the report be shared with OECD and that the FATF Secretariat should facilitate this contact in order to help the FATF develop specific areas where guidance may be needed.

K. FIGHTING TERRORIST FINANCING AND MONEY LAUNDERING

22.	Report by the WGTM Co-chairs	FATF/PLEN/RD(2013)9

Decisions taken:

- The Report by the WGTM Co-Chairs was adopted.

- The Plenary thanked Chip Poncy for his contribution to WGTM work, and welcomed Jennifer Fowler as the new WGTM Co-Chair.

Important issues raised:

- **New payment products and services:** Hong Kong, China supported the consolidated guidance paper. Switzerland noted that, in the future, some standards may need to be revised in relation to these types of products. India noted that it would like another opportunity to share supervisory experiences for inclusion in the paper.

- **Non-profit organisations:** the US, Canada and Spain emphasised the importance of managing expectations, and being clear that, at this stage, there will only be a very limited revision of the best practices paper (BPP). The objective of the dialogue meeting with NPOs (to be held in the margins of the April Private Sector Consultative Forum) is to gather information about the sector's vulnerabilities. Although the FATF will hear from NPOs concerning the limited BPP revisions, it is not seeking specific comments on this issue. The President confirmed this understanding and noted that this revision is clear in acknowledging what already exists in the standards (*i.e.*, that the FATF fully respects the vital role that NPOs play). Spain noted that, although this is a limited revision, from a philosophical point of view, it is a very important change because the FATF acknowledges that its standards may be misinterpreted. The US expressed concern that the BPP was leaked to the private sector.

- **Politically exposed persons:** Switzerland suggested postponing adoption of the paper to October. The Netherlands noted that the current text on domestic PEPs does not adequately take into account the private sector feedback received in Madrid in September 2012. The US noted that sufficient progress on this issue had been made to justify getting further input from the private sector. Italy noted that the interpretation of the standards is a matter for FATF (not the private sector).

- **Corruption:** The US suggested sharing the paper with the G20 Anti-Corruption Working Group to get input and ensure that the document is a useful tool for anti-corruption experts.

- **Work plan:** Canada noted that, in the interests of prioritising FATF work, consideration should be given as to whether it is necessary to undertake all of the BPPs and guidance papers currently listed on the WGTM work plan.

L. THE GLOBAL FATF/FSRB NETWORK

23.	Report by the Global Network Co-ordination Group Co-chairs	FATF/PLEN/RD(2013)10

Decisions taken:

- The Report by the GNCG Co-Chairs was adopted.

Important issues raised:

- The GNCG Co-Chairs reminded delegations of the nature of GNCG Best Practices, which are different from other FATF Best Practices (Papers). GNCG Best Practices are compilations of information that the bodies of the network can use to learn from each other's experiences, and not a prescriptive example of a single best practice.

- The APG raised the importance of the coordination of FATF and FSRB mutual evaluation and follow-up procedures among each other, and with the FATF ICRG procedures. The APG suggested that this issue be discussed at the next FATF meeting in Oslo, Norway.

- CFATF reassured delegations of its financial solvability.

M. CORRUPTION

24.	Consolidated update by the President on FATF work related to corruption	FATF/PLEN(2013)13

Decisions taken:

- The Plenary heard the Consolidated update by the President on FATF work related to corruption.

Important issues raised:

- The Vice-President proposed to hold another Experts Meeting on Corruption in October 2013 in Paris, in the margins of the FATF Plenary and the G20 Anti-Corruption Working Group (ACWG) meeting. This will be an opportunity to leverage the fact that the Russian Federation holds both the FATF and G20 presidencies, and is Co-Chair of the G20 ACWG. It will also help to ensure that the Corruption Best Practices Paper is a useful tool for anti-corruption experts.

- The President noted that this is a welcome sign of the priority that this work should have in FATF.

- Canada noted that, as Co-Chair of the G20 ACWG, it looks forward to working with the Russian Presidency and advancing these issues further.

N. FATF VICE PRESIDENCY

The President explained that an FATF member had expressed interest in taking on this role, but was not yet in a position to confirm. Delegations will be informed by email if a confirmation is received and will be asked to approve or object by email. The formal decision may however be postponed to the next plenary.

O. ANY OTHER BUSINESS

The Executive Secretary, the President and the Plenary offered theirthanks to Mr. Chip Poncy, the head of the US delegation, for the large contribution he has made to the FATF since the year 2000 and wished him well in his new career.

FATF

Methodology

FOR ASSESSING TECHNICAL COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS

February 2013

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

METHODOLOGY

FOR ASSESSING TECHNICAL COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS

FEBRUARY 2013

Printed February 2013

CONTENTS

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for *Combating the financing of terrorism*)
BNI	Bearer-Negotiable Instrument
CDD	Customer Due Diligence
CFT	Countering the financing of terrorism
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IO	Immediate Outcome
IN	Interpretive Note
ML	Money Laundering
MOU	Memorandum of Understanding
MVTS	Money or Value Transfer Service(s)
NPO	Non-Profit Organisation
Palermo Convention	The United Nations Convention against Transnational Organized Crime 2000
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-Based Approach
SRB	Self-Regulating Bodies
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
Terrorist Financing Convention	The International Convention for the Suppression of the Financing of Terrorism 1999
TF	Terrorist Financing
UN	United Nations
UNSCR	United Nations Security Council Resolutions
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

INTRODUCTION

1. This document provides the basis for undertaking assessments of technical compliance with the revised FATF Recommendations, adopted in February 2012, and for reviewing the level of effectiveness of a country's Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) system. It consists of three sections. This first section is an introduction, giving an overview of the assessment Methodology[1], its background, and how it will be used in evaluations/assessments. The second section sets out the criteria for assessing technical compliance with each of the FATF Recommendations. The third section sets out the outcomes, indicators, data and other factors used to assess the effectiveness of the implementation of the FATF Recommendations. The processes and procedures for Mutual Evaluations are set out in a separate document.

2. For its 4th round of mutual evaluations, the FATF has adopted complementary approaches for assessing technical compliance with the FATF Recommendations, and for assessing whether and how the AML/CFT system is effective. Therefore, the Methodology comprises two components:

- The technical compliance assessment addresses the specific requirements of the FATF Recommendations, principally as they relate to the relevant legal and institutional framework of the country, and the powers and procedures of the competent authorities. These represent the fundamental building blocks of an AML/CFT system.
- The effectiveness assessment differs fundamentally from the assessment of technical compliance. It seeks to assess the adequacy of the implementation of the FATF Recommendations, and identifies the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system. The focus of the effectiveness assessment is therefore on the extent to which the legal and institutional framework is producing the expected results.

3. Together, the assessments of both technical compliance and effectiveness will present an integrated analysis of the extent to which the country is compliant with the FATF Standards and how successful it is in maintaining a strong AML/CFT system, as required by the FATF Recommendations.

4. This Methodology is designed to assist assessors when they are conducting an assessment of a country's compliance with the international AML/CFT standards. It reflects the requirements set out in the FATF Recommendations and Interpretive Notes, which constitute the international standard to combat money laundering and the financing of terrorism and proliferation, but does not amend or override them. It will assist assessors in identifying the systems and mechanisms developed by

[1] The terms "assessment", "evaluation" and their derivatives are used throughout this document, and refer to both mutual evaluations undertaken by the FATF and FSRBs and third-party assessments (*i.e.* assessments undertaken by the IMF and World Bank).

countries with diverse legal, regulatory and financial frameworks in order to implement effective AML/CFT systems; and is also useful for countries that are reviewing their own systems, including in relation to technical assistance needs. This Methodology is also informed by the experience of the FATF, the FATF-style regional bodies (FSRBs), the International Monetary Fund and the World Bank in conducting assessments of compliance with earlier versions of the FATF Recommendations.

RISK AND CONTEXT

5. The starting point for every assessment is the assessors' initial understanding of the country's risks and context, in the widest sense, and elements which contribute to them. This includes:

- the nature and extent of the money laundering and terrorist financing risks ;
- the circumstances of the country, which affect the *materiality* of different Recommendations (*e.g.,* the makeup of its economy and its financial sector);
- *structural elements* which underpin the AML/CFT system; and
- *other contextual factors* which could influence the way AML/CFT measures are implemented and how effective they are.

6. The ML/TF *risks* are critically relevant to evaluating technical compliance with Recommendation 1 and the risk-based elements of other Recommendations, and to assess effectiveness. Assessors should consider the nature and extent of the money laundering and terrorist financing risk factors to the country at the outset of the assessment, and throughout the assessment process. Relevant factors can include the level and type of proceeds-generating crime in the country; the terrorist groups active or raising funds in the country; exposure to cross-border flows of criminal or illicit assets.

7. Assessors should use the country's own assessment(s) of its risks as an initial basis for understanding the risks, but should not uncritically accept a country's risk assessment as correct, and need not follow all its conclusions. Assessors should also note the guidance in paragraph 15, below on how to evaluate risk assessments in the context of Recommendation 1 and Immediate Outcome 1. There may be cases where assessors cannot conclude that the country's assessment is reasonable, or where the country's assessment is insufficient or non-existent. In such situations, they should consult closely with the national authorities to try to reach a common understanding of what are the key risks within the jurisdiction. If there is no agreement, or if they cannot conclude that the country's assessment is reasonable, then assessors should clearly explain any differences of understanding, and their reasoning on these, in the Mutual Evaluation Report (MER); and should use their understanding of the risks as a basis for assessing the other risk-based elements (e.g. risk-based supervision).

8. Assessors should also consider issues of *materiality*, including, for example, the relative importance of different parts of the financial sector and different DNFBPs; the size, integration and make-up of the financial sector; the relative importance of different types of financial products or institutions; the amount of business which is domestic or cross-border; the extent to which the economy is cash-based; and estimates of the size of the informal sector and/or shadow economy. Assessors should also be aware of population size, the country's level of development, geographical

factors, and trading or cultural links. Assessors should consider the relative importance of different sectors and issues in the assessment of both technical compliance and of effectiveness. The most important and relevant issues to the country should be given more weight when determining ratings for technical compliance, and more attention should be given to the most important areas when assessing effectiveness, as set out below.

9. An effective AML/CFT system normally requires certain *structural elements* to be in place, for example: political stability; a high-level commitment to address AML/CFT issues; stable institutions with accountability, integrity, and transparency; the rule of law; and a capable, independent and efficient judicial system. The lack of such structural elements, or significant weaknesses and shortcomings in the general framework, may significantly hinder the implementation of an effective AML/CFT framework; and, where assessors identify a lack of compliance or effectiveness, missing structural elements may be a reason for this and should be identified in the MER, where relevant.

10. *Other contextual factors* that might significantly influence the effectiveness of a country's AML/CFT measures include the maturity and sophistication of the regulatory and supervisory regime in the country; the level of corruption and the impact of measures to combat corruption; or the level of financial exclusion. Such factors may affect the ML/FT risks and increase or reduce the effectiveness of AML/CFT measures.

11. Assessors should consider the contextual factors above, including the risks, issues of materiality, structural elements, and other contextual factors, to reach a general understanding of the context in which the country's AML/CFT system operates. These factors may influence which issues assessors consider to be material or higher-risk, and consequently will help assessors determine where to focus their attention in the course of an assessment. Some particularly relevant contextual factors are noted in the context of individual immediate outcomes addressed in the effectiveness component of this Methodology. Assessors should be cautious regarding the information used when considering how these risk and contextual factors might affect a country's evaluation, particularly in cases where they materially affect the conclusions. Assessors should take the country's views into account, but should review them critically, and should also refer to other credible or reliable sources of information (e.g. from international institutions or major authoritative publications), preferably using multiple sources. Based on these elements the assessors should make their own judgement of the context in which the country's AML/CFT system operates, and should make this analysis clear and explicit in the MER.

12. Risk, materiality, and structural or contextual factors may in some cases explain why a country is compliant or non-compliant, or why a country's level of effectiveness is higher or lower than might be expected, on the basis of the country's level of technical compliance. These factors may be an important part of the explanation why the country is performing well or poorly, and an important element of assessors' recommendations about how effectiveness can be improved. Ratings of both technical compliance and effectiveness are judged on a universal standard applied to all countries. An unfavourable context (*e.g.,* where there are missing structural elements), may undermine compliance and effectiveness. However, risks and materiality, and structural or other contextual factors should not be an excuse for poor or uneven implementation of the FATF

standards. Assessors should make clear in the MER which factors they have taken into account; why and how they have done so, and the information sources used when considering them.

GENERAL INTERPRETATION AND GUIDANCE

13. A full set of definitions from the FATF Recommendations are included in the Glossary which accompanies the Recommendations. Assessors should also take note of the following guidance on other points of general interpretation, which is important to ensure consistency of approach.

14. **Financial Institutions** –Assessors should have a thorough understanding of the types of entities that engage in the financial activities referred to in the glossary definition of *financial institutions*. It is important to note that such activities may be undertaken by institutions with different generic names (*e.g.,* "bank") in different countries, and that assessors should focus on the activity, not the names attached to the institutions.

15. **Evaluating the country's Assessment of risk** – Assessors are not expected to conduct an independent risk assessment of their own when assessing Recommendation1 and Immediate Outcome 1, but on the other hand should not necessarily accept a country's risk assessment as correct. In reviewing the country's risk assessment, assessors should consider the rigour of the processes and procedures employed; and the internal consistency of the assessment (*i.e.* whether the conclusions are reasonable given the information and analysis used). Assessors should focus on high-level issues, not fine details, and should take a common-sense approach to whether the results are reasonable. Where relevant and appropriate, assessors should also consider other credible or reliable sources of information on the country's risks, in order to identify whether there might be any material differences that should be explored further. Where the assessment team considers the country's assessment of the risks to be reasonable the risk-based elements of the Methodology could be considered on the basis of it.

16. When assessing Recommendation 1, assessors should concentrate their analysis on the following elements: (1) processes and mechanisms in place to produce and coordinate the risk assessment(s); (2) the reasonableness of the risk assessment(s); and, (3) the alignment of risk-based measures with the risks identified (*e.g.,* exemptions, higher or lower risks situations).

17. When assessing Immediate Outcome 1, assessors, based on their views of the reasonableness of the assessment(s) of risks, should focus on how well the competent authorities use their understanding of the risks in practice to inform policy development and activities to mitigate the risks.

18. **Risk-based requirements** - For each Recommendation where financial institutions and Designated Non-Financial Businesses or Professions (DNFBPs) should be required to take certain actions, assessors should normally assess compliance on the basis that all financial institutions and DNFBPs should have to meet all the specified requirements. However, an important consideration underlying the FATF Recommendations is the degree of risk of money laundering or terrorist financing for particular types of institutions, businesses or professions, or for particular customers, products, transactions, or countries. A country may, therefore, take risk into account in the application of the Recommendations (*e.g.,* in the application of simplified measures), and assessors

will need to take the risks, and the flexibility allowed by the risk-based approach, into account when determining whether there are deficiencies in a country's preventive measures, and their importance. Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, all such measures must be applied, although the extent of such measures may vary according to the specific level of risk.

19. **Exemptions for low-risk situations** – Where there is a low risk of money laundering and terrorist financing, countries may decide not to apply some of the Recommendations requiring financial institutions and DNFBPs to take certain actions. In such cases, countries should provide assessors with the evidence and analysis which was the basis for the decision not to apply the Recommendations.

20. **Requirements for financial institutions, DNFBPs, and countries** - The FATF Recommendations state that financial institutions or DNFBPs "*should*" or "*should be required to*" take certain actions, or that countries "*should ensure*" that certain actions are taken by financial institutions, DNFBPs or other entities or persons. In order to use one consistent phrase, the relevant criteria in this Methodology use the phrase "*Financial institutions (or DNFBPs) should be required*".

21. **Law or enforceable means** – The note on the *Legal basis of requirements on financial institutions and DNFBPs* (at the end of the Interpretive Notes to the FATF Recommendations) sets out the required legal basis for enacting the relevant requirements. Assessors should consider whether the mechanisms used to implement a given requirement qualify as an *enforceable means* on the basis set out in that note. Assessors should be aware that Recommendations 10, 11, and 20 contain requirements which must be set out in law, while other requirements may be set out in either law or enforceable means. It is possible that types of documents or measures which are not considered to be enforceable means may nevertheless help contribute to effectiveness, and may, therefore, be considered in the context of effectiveness analysis, without counting towards meeting requirements of technical compliance (*e.g.,* voluntary codes of conduct issued by private sector bodies or non-binding guidance by a supervisory authority).

22. **Assessment for DNFBPs** – Under Recommendations 22, 23 and 28 (and specific elements of Recommendations 6 and 7), DNFBPs and the relevant supervisory (or self-regulatory) bodies are required to take certain actions. Technical compliance with these requirements should only be assessed under these specific Recommendations and should not be carried forward into other Recommendations relating to financial institutions. However, the assessment of effectiveness should take account of both financial institutions and DNFBPs when examining the relevant outcomes.

23. **Financing of Proliferation** – The requirements of the FATF Standard relating to the financing of proliferation are limited to Recommendation 7 ("Targeted Financial Sanctions") and Recommendation 2 ("National Co-operation and Co-ordination"). In the context of the effectiveness assessment, all requirements relating to the financing of proliferation are included within Outcome 11, except those on national co-operation and co-ordination, which are included in Immediate Outcome 1. Issues relating to the financing of proliferation should be considered in those places only, and not in other parts of the assessment.

24. **National, supra-national and sub-national measures** - In some countries, AML/CFT issues are addressed not just at the level of the national government, but also at state/province or local

levels. When assessments are being conducted, appropriate steps should be taken to ensure that AML/CFT measures at the state/provincial level are also adequately considered. Equally, assessors should take into account and refer to supra-national laws or regulations that apply to a country. Annex I sets out the specific Recommendations that may be assessed on a supra-national basis.

25. **Financial Supervision** – Laws and enforceable means that impose preventive AML/CFT requirements upon the banking, insurance, and securities sectors should be implemented and enforced through the supervisory process. In these sectors, the relevant core supervisory principles issued by the Basel Committee, IAIS, and IOSCO should also be adhered to. For certain issues, these supervisory principles will overlap with or be complementary to the requirements set out in the FATF standards. Assessors should be aware of, and have regard to, any assessments or findings made with respect to the Core Principles, or to other relevant principles or standards issued by the supervisory standard-setting bodies. For other types of financial institutions, it will vary from country to country as to whether these laws and obligations are implemented and enforced through a regulatory or supervisory framework, or by other means.

26. **Sanctions** – Several Recommendations require countries to have "*effective, proportionate, and dissuasive sanctions*" for failure to comply with AML/CFT requirements. Different elements of these requirements are assessed in the context of technical compliance and of effectiveness. In the technical compliance assessment, assessors should consider whether the country's framework of laws and enforceable means includes a sufficient range of sanctions that they can be applied *proportionately* to greater or lesser breaches of the requirements[2]. In the effectiveness assessment, assessors should consider whether the sanctions applied in practice are *effective* at ensuring future compliance by the sanctioned institution; and *dissuasive* of non-compliance by others.

27. **International Co-operation** – In this Methodology, international co-operation is assessed in specific Recommendations and Immediate Outcomes (principally Recommendations 36-40 and Immediate Outcome 2). Assessors should also be aware of the impact that a country's ability and willingness to engage in international co-operation may have on other Recommendations and Immediate Outcomes (*e.g.,* on the investigation of crimes with a cross-border element or the supervision of international groups), and set out clearly any instances where compliance or effectiveness is positively or negatively affected by international co-operation.

28. **Draft legislation and proposals** – Assessors should only take into account relevant laws, regulations or other AML/CFT measures that are in force and effect by the end of the on-site visit to the country. Where bills or other specific proposals to amend the system are made available to assessors, these may be referred to in the report, but should not be taken into account in the conclusions of the assessment or for ratings purposes.

[2] Examples of types of sanctions include: written warnings; orders to comply with specific instructions (possibly accompanied with daily fines for non-compliance); ordering regular reports from the institution on the measures it is taking; fines for non-compliance; barring individuals from employment within that sector; replacing or restricting the powers of managers, directors, and controlling owners; imposing conservatorship or suspension or withdrawal of the license; or criminal penalties where permitted.

29. **FATF Guidance** - assessors may also consider FATF Guidance as background information on how countries can implement specific requirements. A full list of FATF Guidance is included as an annex to this document. Such guidance may help assessors understand the practicalities of implementing the FATF Recommendations, but the application of the guidance should not form part of the assessment.

TECHNICAL COMPLIANCE

30. The technical compliance component of the Methodology refers to the implementation of the specific requirements of the FATF Recommendations, including the framework of laws and enforceable means; and the existence, powers and procedures of competent authorities. For the most part, it does not include the specific requirements of the standards that relate principally to effectiveness. These are assessed separately, through the effectiveness component of the Methodology.

31. The FATF Recommendations, being the recognised international standards, are applicable to all countries. However, assessors should be aware that the legislative, institutional and supervisory framework for AML/CFT may differ from one country to the next. Provided the FATF Recommendations are complied with, countries are entitled to implement the FATF Standards[3] in a manner consistent with their national legislative and institutional systems, even though the methods by which compliance is achieved may differ. In this regard, assessors should be aware of the risks, and the structural or contextual factors for the country.

32. The technical compliance component of the Methodology sets out the specific requirements of each Recommendation as a list of criteria, which represent those elements that should be present in order to demonstrate full compliance with the mandatory elements of the Recommendations. Criteria to be assessed are numbered sequentially for each Recommendation, but the sequence of criteria does not represent any priority or order of importance. In some cases, elaboration (indented below the criteria) is provided in order to assist in identifying important aspects of the assessment of the criteria. For criteria with such elaboration, assessors should review whether each of the elements is present, in order to judge whether the criterion as a whole is met.

COMPLIANCE RATINGS

33. For each Recommendation assessors should reach a conclusion about the extent to which a country complies (or not) with the standard. There are four possible levels of compliance: compliant, largely compliant, partially compliant, and non-compliant. In exceptional circumstances, a Recommendation may also be rated as not applicable. These ratings are based only on the criteria specified in the technical compliance assessment, and are as follows:

[3] The FATF Standards comprise the FATF Recommendations and their Interpretive Notes.

Technical compliance ratings		
Compliant	C	There are no shortcomings.
Largely compliant	LC	There are only minor shortcomings.
Partially compliant	PC	There are moderate shortcomings.
Non-compliant	NC	There are major shortcomings.
Not applicable	NA	A requirement does not apply, due to the structural, legal or institutional features of a country.

When deciding on the level of shortcomings for any Recommendation, assessors should consider, having regard to the country context, the number and the relative importance of the criteria met or not met.

34. It is essential to note that it is the responsibility of the assessed country to demonstrate that its AML/CFT system is compliant with the Recommendations. In determining the level of compliance for each Recommendation, the assessor should not only assess whether laws and enforceable means are compliant with the FATF Recommendations, but should also assess whether the institutional framework is in place.

35. **Weighting** – The individual criteria used to assess each Recommendation do not all have equal importance, and the number of criteria met is not always an indication of the overall level of compliance with each Recommendation. When deciding on the rating for each Recommendation, assessors should consider the relative importance of the criteria in the context of the country. Assessors should consider how significant any deficiencies are given the country's risk profile and other structural and contextual information (*e.g.,* for a higher risk area or a large part of the financial sector). In some cases a single deficiency may be sufficiently important to justify an NC rating, even if other criteria are met. Conversely a deficiency in relation to a low risk or little used types of financial activity may have only a minor effect on the overall rating for a Recommendation.

36. **Overlaps between Recommendations** – In many cases the same underlying deficiency will have a cascading effect on the assessment of several different Recommendations. For example: a deficient risk assessment could undermine risk-based measures throughout the AML/CFT system; or a failure to apply AML/CFT regulations to a particular type of financial institution or DNFBP could affect the assessment of all Recommendations which apply to financial institutions or DNFBPs. When considering ratings in such cases, assessors should reflect the deficiency in the factors underlying the rating for each applicable Recommendation, and, if appropriate, mark the rating accordingly. They should also clearly indicate in the MER that the same underlying cause is involved in all relevant Recommendations.

37. **Comparison with previous ratings** - Due to the revision and consolidation of the FATF Recommendations and Special Recommendations in 2012, and the introduction of separate assessments for technical compliance and effectiveness, the ratings given under this Methodology will not be directly comparable with ratings given under the 2004 Methodology.

EFFECTIVENESS

38. The assessment of the effectiveness of a country's AML/CFT system is equally as important as the assessment of technical compliance with the FATF standards. Assessing effectiveness is intended to: (a) improve the FATF's focus on outcomes; (b) identify the extent to which the national AML/CFT system is achieving the objectives of the FATF standards, and identify any systemic weaknesses; and (c) enable countries to prioritise measures to improve their system. For the purposes of this Methodology, effectiveness is defined as "*The extent to which the defined outcomes are achieved*".

39. In the AML/CFT context, effectiveness is the extent to which financial systems and economies mitigate the risks and threats of money laundering, and financing of terrorism and proliferation. This could be in relation to the intended result of a given (a) policy, law, or enforceable means; (b) programme of law enforcement, supervision, or intelligence activity; or (c) implementation of a specific set of measures to mitigate the money laundering and financing of terrorism risks, and combat the financing of proliferation.

40. The goal of an assessment of effectiveness is to provide an appreciation of the whole of the country's AML/CFT system and how well it works. Assessing effectiveness is based on a fundamentally different approach to assessing technical compliance with the Recommendations. It does not involve checking whether specific requirements are met, or that all elements of a given Recommendation are in place. Instead, it requires a judgement as to whether, or to what extent defined outcomes are being achieved, *i.e.* whether the key objectives of an AML/CFT system, in line with the FATF Standards, are being effectively met in practice The assessment process is reliant on the judgement of assessors, who will work in consultation with the assessed country.

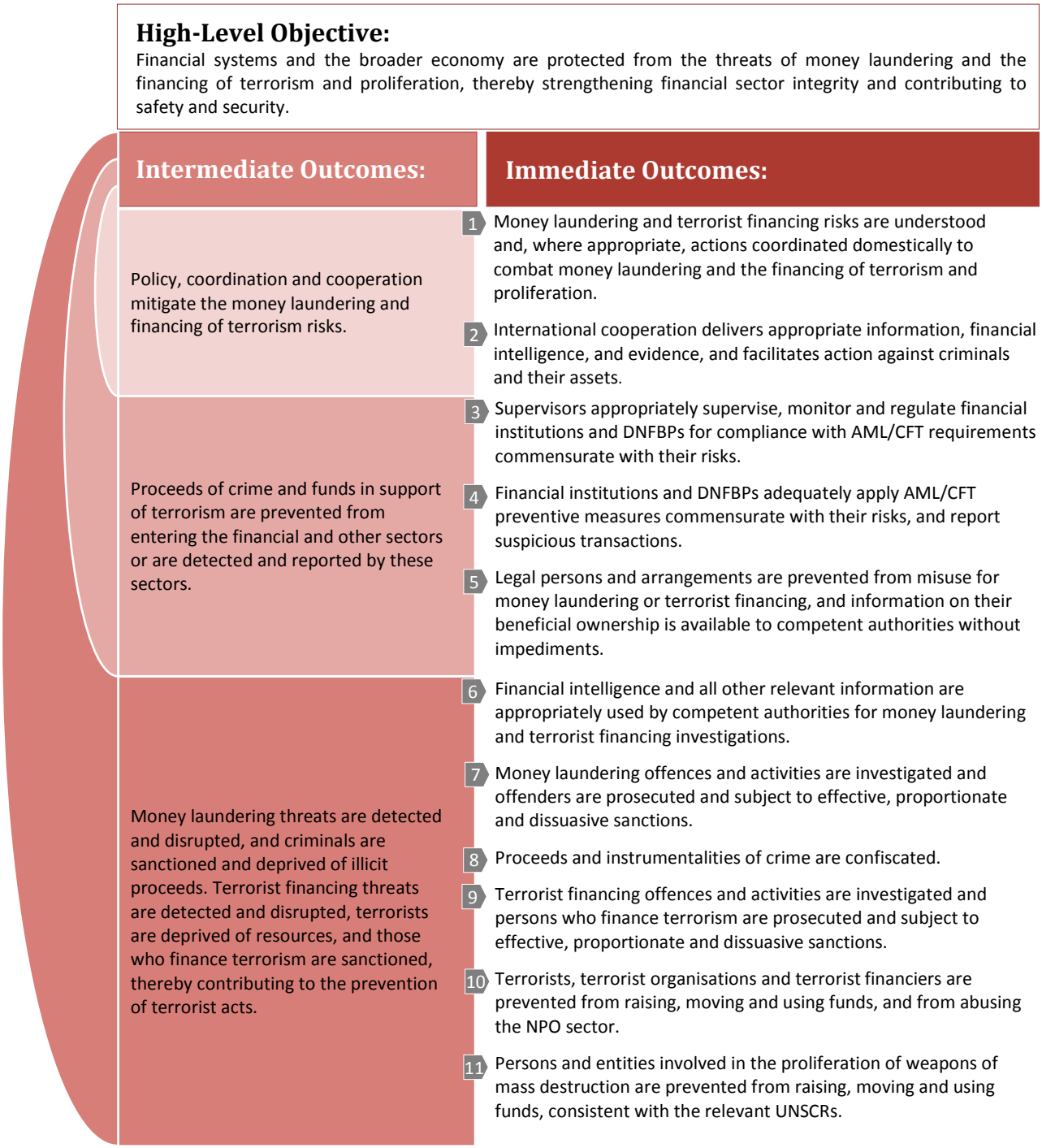
41. It is essential to note that it is the responsibility of the assessed country to demonstrate that its AML/CFT system is effective. If the evidence is not made available, assessors can only conclude that the system is not effective.

THE FRAMEWORK FOR ASSESSING EFFECTIVENESS

42. For its assessment of effectiveness, the FATF has adopted an approach focusing on a hierarchy of defined outcomes. At the highest level, the objective in implementing AML/CFT measures is that "*Financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security*". In order to give the right balance between an overall understanding of the effectiveness of a country's AML/CFT system, and a detailed appreciation of how well its component parts are operating, the FATF assesses effectiveness primarily on the basis of *eleven Immediate Outcomes*. Each of these represents one of the key goals which an effective AML/CFT system should achieve, and they feed into three Intermediate Outcomes which represent the major thematic goals of AML/CFT measures. This approach does not seek to assess directly the effectiveness with which a country is implementing individual Recommendations; or the performance of specific organisations, or institutions. Assessors are not expected to evaluate directly

the High-Level Objective or Intermediate Outcomes, though these could be relevant when preparing the written MER and summarising the country's overall effectiveness in general terms.

43. The relation between the High-Level Objective, the Intermediate Outcomes, and the Immediate Outcomes, is set out in the diagram below:



SCOPING

44. Assessors must assess all eleven of the Immediate Outcomes. However, prior to the on-site visit, assessors should conduct a scoping exercise, in consultation with the assessed country, which should take account of the risks and other factors set out in paragraphs 5 to 10 above. Assessors should, in consultation with the assessed country, identify the higher risk issues, which should be examined in more detail in the course of the assessment and reflected in the final report. They should also seek to identify areas of lower/low risk, which may not need to be examined in the same level of detail. As the assessment continues, assessors should continue to engage the country and review their scoping based on their initial findings about effectiveness, with a view to focusing their attention on the areas where there is greatest scope to improve effectiveness in addressing the key ML/TF risks.

LINKS TO TECHNICAL COMPLIANCE

45. The country's level of technical compliance contributes to the assessment of effectiveness. Assessors should consider the level of technical compliance as part of their scoping exercise. The assessment of technical compliance reviews whether the legal and institutional foundations of an effective AML/CFT system are present. It is unlikely that a country that is assessed to have a low level of compliance with the technical aspects of the FATF Recommendations will have an effective AML/CFT system (though it cannot be taken for granted that a technically compliant country will also be effective). In many cases, the main reason for poor effectiveness will be serious deficiencies in implementing the technical elements of the Recommendations.

46. In the course of assessing effectiveness, assessors should also consider the impact of technical compliance with the relevant Recommendations when explaining why the country is (or is not) effective and making recommendations to improve effectiveness. There may in exceptional circumstances be situations in which assessors conclude that there is a low level of technical compliance but nevertheless a certain level of effectiveness (*e.g.,* as a result of specific country circumstances, including low risks or other structural, material or contextual factors; particularities of the country's laws and institutions; or if the country applies compensatory AML/CFT measures which are not required by the FATF Recommendations). Assessors should pay particular attention to such cases in the MER, and must fully justify their decision, explaining in detail the basis and the specific reasons for their conclusions on effectiveness, despite lower levels of technical compliance.

USING THE EFFECTIVENESS METHODOLOGY

47. An assessment of effectiveness should consider each of the eleven Immediate Outcomes individually, but does not directly focus on the Intermediate or High-Level Outcomes. For each of the Immediate Outcomes, there are two overarching questions which assessors should try to answer:

- ***To what extent is the outcome being achieved?*** Assessors should assess whether the country is effective in relation to that outcome (*i.e.* whether the country is achieving the results expected of a well-performing AML/CFT system). They should base their conclusions principally on the *Core Issues*,

supported by the *examples of information* and the *examples of specific factors*; and taking into account the level of technical compliance, and contextual factors.

- ***What can be done to improve effectiveness?*** Assessors should understand the reasons why the country may not have reached a high level of effectiveness and, where possible, make recommendations to improve its ability to achieve the specific outcome. They should base their analysis and recommendations on their consideration of the *core issues* and on the *examples of specific factors that could support the conclusions on core issues*, including activities, processes, resources and infrastructure. They should also consider the effect of technical deficiencies on effectiveness, and the relevance of contextual factors. If assessors are satisfied that the outcome is being achieved to a high degree, they would not need to consider in detail *what can be done to improve effectiveness* (though there may still be value in identifying good practises or potential further improvements, or ongoing efforts needed to sustain a high level of effectiveness).

Characteristics of an Effective System

48. The boxed text at the top of each of the Immediate Outcomes describes the main features and outcomes of an effective system. This sets out the situation in which a country is effective at achieving the outcome, and provides the benchmark for the assessment.

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

49. The second section sets out the basis for assessors to judge if, and to what extent, the outcome is being achieved. The *core issues* are the mandatory questions which assessors should seek to answer, in order to get an overview about how effective a country is under each outcome. Assessors' conclusions about how effective a country is should be based on an overview of each outcome, informed by the assessment of the *core issues*.

50. Assessors should examine all the *core issues* listed for each outcome. However, they may vary the degree of detail with which they examine each in order to reflect the degree of risk and materiality associated with that issue in the country. In exceptional circumstances, assessors may also consider additional issues which they consider, in the specific circumstances, to be core to the effectiveness outcome (*e.g.,* alternative measures which reflect the specificities of the country's AML/CFT system, but which are not included in the *core issues* or as additional *information* or *specific factors*). They should make clear when, and why, any additional issues have been used which are considered to be core.

Examples of information that could support the conclusions on Core Issues

51. The *Examples of Information* sets out the types and sources of information which are most relevant to understanding the extent to which the outcome is achieved, including particular data

points which assessors might look for when assessing the *core issues*. The supporting information and other data can test or validate assessors' understanding of the core issues, and can provide a quantitative element to complete the assessors' picture of how well the outcome is achieved.

52. The supporting information and data listed are not exhaustive and not mandatory. The data, statistics, and other material which are available will vary considerably from country to country, and assessors should make use of whatever information the country can provide in order to assist in reaching their judgement.

53. Assessment of effectiveness is not a statistical exercise. Assessors should use data and statistics, as well as other qualitative information, when reaching an informed judgement about how well the outcome is being achieved, but should interpret the available data critically, in the context of the country's circumstances. The focus should not be on raw data (which can be interpreted in a wide variety of ways and even with contradictory conclusions), but on information and analysis which indicates, in the context of the country being assessed, whether the objective is achieved. Assessors should be particularly cautious about using data relating to other countries as a comparison point in judging effectiveness, given the significant differences in country circumstances, AML/CFT systems, and data collection practices. Assessors should also be aware that a high level of outputs does not always contribute positively towards achieving the desired outcome.

Examples of specific factors that could support the conclusions on core issues

54. The *factors* section of the Methodology sets out examples of the elements which are normally involved in delivering each outcome. These are not an exhaustive list of the possible factors, but are provided as an aid to assessors when considering the reasons why a country may (or may not) be achieving a particular outcome (*e.g.,* through a breakdown in one of the factors). In most cases, assessors will need to refer to the *factors* in order to reach a firm conclusion about the extent to which a particular outcome is being achieved. It should be noted that the activities and processes listed in this section do not imply a single mandatory model for organising AML/CFT functions, but only represent the most commonly implemented administrative arrangements, and that the reasons why a country may not be effective are not limited to the factors listed. It should be noted that assessors need to focus on the qualitative aspects of these *factors*, not on the mere underlying process or procedure.

55. Assessors are not required to review all the *factors* in every case. When a country is demonstrably effective in an area, assessors should set out succinctly why this is the case, and highlight any areas of particular good practice, but they do not need to examine every individual factor in this section of the Methodology. There may also be cases in which a country is demonstrably not effective and where the reasons for this are fundamental (*e.g.,* where there are major technical deficiencies). In such cases, there is also no need for assessors to undertake further detailed examination of why the outcome is not being achieved.

56. Assessors should be aware of outcomes which depend on a sequence of different steps, or a *value-chain* to achieve the outcome (*e.g.,* Immediate Outcome 7, which includes investigation, prosecution and sanctioning, in order). In these cases, it is possible that an outcome may not be

achieved because of a failure at one stage of the process, even though the other stages are themselves effective.

57. Assessors should also consider contextual factors, which may influence the issues assessors consider to be material or higher risk, and consequently, where they focus their attention. These factors may be an important part of the explanation why the country is performing well or poorly, and an important element of assessors' recommendations about how effectiveness can be improved. However, they should not be an excuse for poor or uneven implementation of the FATF standards.

CROSS-CUTTING ISSUES

58. The Immediate Outcomes are not independent of each other. In many cases an issue considered specifically under one Immediate Outcome will also contribute to the achievement of other outcomes. In particular, the factors assessed under Immediate Outcomes 1 and 2, which consider (a) the country's assessment of risks and implementation of the risk-based approach; and (b) its engagement in international co-operation, may have far-reaching effects on other outcomes (*e.g.,* risk assessment affects the application of risk-based measures under Immediate Outcome 4, and the deployment of competent authorities' resources relative to all outcomes; international co-operation includes seeking co-operation to support domestic ML investigations and confiscation proceedings under Immediate Outcomes 7 and 8). Therefore, assessors should take into consideration how their findings for Immediate Outcomes 1 and 2 may have a positive or negative impact on the level of effectiveness for other Immediate Outcomes. These cross-cutting issues are reflected in the *notes to assessors* under each Immediate Outcome.

CONCLUSIONS ON EFFECTIVENESS

59. For each individual Immediate Outcome, assessors should reach conclusions about the extent to which a country is (or is not) effective. In cases where the country has not reached a high level of effectiveness, assessors should also make recommendations about the reasons why this is the case, and the measures which the country should take to improve its ability to achieve the outcome.

60. ***Effectiveness is assessed in a fundamentally different way to technical compliance***. Assessors' conclusions about the extent to which a country is more or less effective should be based on an overall understanding of the degree to which the country is achieving the outcome. ***The Core Issues should <u>not</u> be considered as a checklist of criteria***, but as a set of questions which help assessors achieve an appropriate understanding of the country's effectiveness for each of the Immediate Outcomes. The core issues are not equally important, and their significance will vary according to the specific situation of each country, taking into account the ML/TF risks and relevant structural factors. Therefore, assessors need to be flexible and to use their judgement and experience when reaching conclusions.

61. Assessors' conclusions should reflect only *whether the outcome is being achieved*. Assessors should set-aside their own preferences about the best way to achieve effectiveness, and should not be unduly influenced by their own national approach. They should also avoid basing their conclusions on the number of problems or deficiencies identified, as it is possible that a country may

have several weaknesses which are not material in nature or are offset by strengths in other areas, and is therefore able to achieve a high overall level of effectiveness.

62. ***Assessors' conclusions on the level of effectiveness should be primarily descriptive***. Assessors should set out clearly the extent to which they consider the outcome to be achieved overall, noting any variation, such as particular areas where effectiveness is higher or lower. They should also clearly explain the basis for their judgement, *e.g.,* problems or weaknesses which they believe are responsible for a lack of effectiveness; the *core issues* and the information which they considered to be most significant; the way in which they understood data and other indicators; and the weight they gave to different aspects of the assessment. Assessors should also identify any areas of particular strength or examples of good practice.

63. In order to ensure clear and comparable decisions, assessors should also summarise their conclusion in the form of a rating. For each Immediate Outcome there are four possible ratings for effectiveness, based on the extent to which the *core issues* and *characteristics* are addressed: *High level of effectiveness; Substantial level of effectiveness; Moderate level of effectiveness; and Low level of effectiveness.* These ratings should be decided on the basis of the following:

Effectiveness ratings	
High level of effectiveness	The Immediate Outcome is achieved to a very large extent. Minor improvements needed.
Substantial level of effectiveness	The Immediate Outcome is achieved to a large extent. Moderate improvements needed.
Moderate level of effectiveness	The Immediate Outcome is achieved to some extent. Major improvements needed.
Low level of effectiveness	The Immediate Outcome is not achieved or achieved to a negligible extent. Fundamental improvements needed.

RECOMMENDATIONS ON HOW TO IMPROVE THE AML/CFT SYSTEM

64. Assessors' recommendations to a country are a vitally important part of the evaluation. On the basis of their conclusions, assessors should make recommendations of measures that the country should take in order to improve its AML/CFT system, including both the level of effectiveness and the level of technical compliance. The report should prioritise these recommendations for remedial measures, taking into account the country's circumstances and capacity, its level of effectiveness, and any weaknesses and problems identified. Assessors' recommendations should not simply be to address each of the deficiencies or weaknesses identified, but should add value by identifying and prioritising specific measures in order to most effectively mitigate the risks the country faces. This

could be on the basis that they offer the greatest and most rapid practical improvements, have the widest-reaching effects, or are easiest to achieve.

65. Assessors should be careful to consider the circumstances and context of the country, and its legal and institutional system when making recommendations, noting that there are several different ways to achieve an effective AML/CFT system, and that their own preferred model may not be appropriate in the context of the country assessed.

66. In order to facilitate the development of an action plan by the assessed country, assessors should clearly indicate in their recommendations where a specific action is required, and where there may be some flexibility about how a given priority objective is to be achieved. Assessors should avoid making unnecessarily rigid recommendations (*e.g.,* on the scheduling of certain measures), so as not to hinder countries efforts to fully adapt the recommendations to fit local circumstances.

67. Even if a country has a high level of effectiveness, this does not imply that there is no further room for improvement. There may also be a need for action in order to sustain a high level of effectiveness in the face of evolving risks. If assessors are able to identify further actions in areas where there is a high degree of effectiveness, then they should also include these in their recommendations.

POINT OF REFERENCE

68. If assessors have any doubts about how to apply this Methodology, or about the interpretation of the FATF Standards, they should consult the FATF Secretariat or the Secretariat of their FSRB.

TECHNICAL COMPLIANCE ASSESSMENT

RECOMMENDATION 1 ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH[4]

OBLIGATIONS AND DECISIONS FOR COUNTRIES

Risk assessment

1.1 Countries[5] should identify and assess the ML/TF risks for the country,

1.2 Countries should designate an authority or mechanism to co-ordinate actions to assess risks.

1.3 Countries should keep the risk assessments up-to-date.

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.

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.

---

4 The requirements in this recommendation should be assessed taking into account the more specific risk based requirements in other Recommendations. Under Recommendation 1 assessors should come to an overall view of risk assessment and risk mitigation by countries and financial institutions/DNFBPs as required in other Recommendations, but should not duplicate the detailed assessments of risk-based measures required under other Recommendations. Assessors are not expected to conduct an in-depth review of the country's assessment(s) of risks. Assessors should focus on the process, mechanism, and information sources adopted by the country, as well as the contextual factors, and should consider the reasonableness of the conclusions of the country's assessment(s) of risks.

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

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[6].

1.9 Supervisors and SRBs should ensure that financial institutions and DNFBPs are implementing their obligations under Recommendation 1[7].

OBLIGATIONS AND DECISIONS FOR FINANCIAL INSTITUTIONS AND DNFBPS

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)[8]. 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:

---

6 Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, countries should ensure that all such measures are applied, although the extent of such measures may vary according to the specific level of risk.

7 The requirements in this criterion should be assessed taking into account the findings in relation to Recommendations 26 and 28.

8 The nature and extent of any assessment of ML/TF risks should be appropriate to the nature and size of the business. Competent authorities or SRBs may determine that individual documented risk assessments are not required, provided that the specific risks inherent to the sector are clearly identified and understood, and that individual financial institutions and DNFBPs understand their ML/TF risks.

(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 CO-OPERATION AND CO-ORDINATION

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 co-ordination or other mechanism that is responsible for national AML/CFT policies.

2.3 Mechanisms should be in place to enable policy makers, the Financial Intelligence Unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities to co-operate, and where appropriate, co-ordinate 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)[9].

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[10].

3.3 Where countries apply a threshold approach or a combined approach that includes a threshold approach[11], 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.

---

9 Note in particular the physical and material elements of the offence.

10 Recommendation 3 does not require countries to create a separate offence of "participation in an organised criminal group and racketeering". In order to cover this category of "designated offence", it is sufficient if a country meets either of the two options set out in the Palermo Convention, *i.e.* either a separate offence or an offence based on conspiracy.

11 Countries determine the underlying predicate offences for ML by reference to (a) all offences; or (b) to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or (c) to a list of predicate offences; or (d) a combination of these approaches.

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[12];

(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.

[12] Measures should allow the initial application to freeze or seize property subject to confiscation to be made *ex-parte* or without prior notice, unless this is inconsistent with fundamental principles of domestic law.

RECOMMENDATION 5 TERRORIST FINANCING OFFENCE

5.1 Countries should criminalise TF on the basis of the Terrorist Financing Convention[13].

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).[14]

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[15].

5.9 TF offences should be designated as ML predicate offences.

---

13 Criminalisation should be consistent with Article 2 of the International Convention for the Suppression of the Financing of Terrorism.

14 Criminalising TF solely on the basis of aiding and abetting, attempt, or conspiracy is not sufficient to comply with the Recommendation.

15 Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a TF offence; or (ii) be made in the knowledge of the intention of the group to commit a TF offence.

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[16]; a statement of case[17] which contains as much detail as possible on the basis for the listing[18]; 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.

---

16 In particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice

17 This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the relevant committee (the 1267/1989 Committee or 1988 Committee).

18 Including: specific information supporting a determination that the person or entity meets the relevant designation; the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity

(b) have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in UNSCR 1373[19];

(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[20]. 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[21].

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:

---

19 This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries pursuant to UNSCR 1373 (2001)

20 A country should apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that "reasonable grounds" or "reasonable basis" exist for a decision to designate a person or entity, and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant country's own motion or at the request of another country.

21 For UNSCR 1373, the obligation to take action without delay is triggered by a designation at the (supra-) national level, as put forward either on the country's own motion or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373.

(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[22] 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.

[22] "or", in this particular case means that countries must both prohibit their own nationals and prohibit any persons/entities in their jurisdiction.

Such procedures and criteria should be in accordance with procedures adopted by the *1267/1989 Committee* or the *1988 Committee*, as appropriate[23];

(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.

---

23 The procedures of the *1267/1989 Committee* are set out in UNSCRs 1730; 1735; 1822; 1904; 1989; 2083 and any successor resolutions. The procedures of the *1988 Committee* are set out in UNSCRs 1730; 1735; 1822; 1904; 1988; 2082; and any successor resolutions.

RECOMMENDATION 7 TARGETED 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.[24].

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 United Nations 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.

---

24 Recommendation 7 is applicable to all current UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future UNSCRs which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Methodology, (February 2013), the UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: S/RES/1718(2006), S/RES/1737(2006), S/RES/1747(2007), S/RES/1803(2008), S/RES/1874(2009), and S/RES/1929(2010).

(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[25]. 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 be subject to these provisions and are frozen; and

[25] Such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the United Nations Security Council pursuant to UNSCR 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution.

(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; and

(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[26];

(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[27], and the information in (a) and (b) above, and make these available to competent authorities upon appropriate authority.

---

26 Specific licensing or registration requirements for AML/CFT purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favourable tax treatment (such as tax credits or tax exemptions).

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[28].

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

(a) domestic co-operation, co-ordination 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.

---

27 Such records should be sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation.

28 The range of such sanctions might include freezing of accounts, removal of trustees, fines, de-certification, de-licensing and de-registration. This should not preclude parallel civil, administrative, or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

RECOMMENDATION 9 FINANCIAL INSTITUTION SECRECY LAWS

9.1 Financial institution secrecy laws should not inhibit the implementation of the FATF Recommendations[29].

[29] Areas where this may be of particular concern are the ability of competent authorities to access information they require to properly perform their functions in combating ML or FT; the sharing of information between competent authorities, either domestically or internationally; and the sharing of information between financial institutions where this is required by Recommendations 13, 16 or 17.

RECOMMENDATION 10 CUSTOMER DUE DILIGENCE[30] (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/EUR 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:

30 The principle that financial institutions conduct CDD should be set out in law, though specific requirements may be set out in enforceable means.

(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[31], 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[32]) who ultimately has a controlling ownership interest[33] 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

[31] Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

[32] Ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership.

[33] A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%).

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[34], 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.

[34] For beneficiaries of trusts that are designated by characteristics or by class, financial institutions should obtain 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 or when the beneficiary intends to exercise vested rights.

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[35] on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Risk-Based Approach

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

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

Failure to satisfactorily complete CDD

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

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

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

35 Existing customers as at the date that the new national requirements are brought into force.

CDD and tipping-off

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

RECOMMENDATION 11 RECORD KEEPING[36]

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.

36 The principle that financial institutions should maintain records on transactions and information obtained through CDD measures should be set out in law.

RECOMMENDATION 12 POLITICALLY EXPOSED PERSONS (PEPS)

12.1 In relation to foreign PEPs, in addition to performing the CDD measures required under Recommendation 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 Recommendation10, 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[37].

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.

[37] Countries need not impose a separate licensing or registration system with respect to licensed or registered financial institutions which are authorised to perform MVTS.

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[38] 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.

[38] "Accurate" is used to describe information that has been verified for accuracy; *i.e.* financial institutions should be required to verify the accuracy of the required originator information.

(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[39], 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.

---

39 This term also refers to any chain of wire transfers that takes place entirely within the borders of the European Union. It is further noted that the European internal market and corresponding legal framework is extended to the members of the European Economic Area.

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[40], 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 Recommendation 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

[40] Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1 000). Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.

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[41] 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.

41 The term *relevant competent authorities* in Recommendation 17 means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities, that should be involved for the branches/subsidiaries.

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[42]

20.1 If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity[43], or are related to TF, it should be required to report promptly its suspicions to the Financial Intelligence Unit.

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

42 The requirement that financial institutions should report suspicious transactions should be set out in law.

43 "Criminal activity" refers to: (a) all criminal acts that would constitute a predicate offence for ML in the country; or (b) at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3.

RECOMMENDATION 21 TIPPING-OFF AND CONFIDENTIALITY

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

21.2 Financial institutions and their directors, officers and employees should be prohibited by law from disclosing the fact that an STR or related information is being filed with the Financial Intelligence Unit.

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[44] 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[45].

(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;
- creating, operating 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;

---

44 Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link CDD information for a particular customer to the transactions that the customer conducts in the casino. "Financial transactions" does not refer to gambling transactions that involve only casino chips or tokens.

45 This means that real estate agents should comply with the requirements set out in Recommendation 10 with respect to both the purchasers and the vendors of the property.

- 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 [46] – 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)[47].

(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[48].

---

46 Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings.

47 Where countries allow lawyers, notaries, other independent legal professionals and accountants to send their STRs to their appropriate self-regulatory bodies (SRBs), there should be forms of co-operation between these bodies and the FIU.

48 Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

RECOMMENDATION 24 TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS[49]

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[50], 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[51].

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.

---

49 Assessors should consider the application of all the criteria to all relevant types of legal persons. The manner in which these requirements are addressed may vary according to the type of legal person involved:

1. *Companies* - The measures required by Recommendation 24 are set out with specific reference to companies.
2. *Foundations, Anstalt, and limited liability partnerships* - countries should take similar measures and impose similar requirements as those required for companies, taking into account their different forms and structures.
3. *Other types of legal persons* - countries should take into account the different forms and structures of those other legal persons, and the levels of ML/TF risks associated with each type of legal person, with a view to achieving appropriate levels of transparency. At a minimum, all legal persons should ensure that similar types of basic information are recorded.

50 The register of shareholders and members can be recorded by the company itself or by a third person under the company's responsibility.

51 In cases in which the company or company registry holds beneficial ownership information within the country, the register of shareholders and members need not be in the country, if the company can provide this information promptly on request.

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 co-operate 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[52], 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

[52] Members of the company's board or senior management may not require specific authorisation by the company.

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;

(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 co-operation 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[53]

25.1 Countries should require:

(a) trustees of any express trust governed under their law[54] 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[55]; 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

---

53 The measures required by Recommendation 25 are set out with specific reference to trusts. This should be understood as referring to express trusts (as defined in the glossary). In relation to other types of legal arrangement with a similar structure or function, countries should take similar measures to those required for trusts, with a view to achieving similar levels of transparency. At a minimum, countries should ensure that information similar to that specified in respect of trusts should be recorded and kept accurate and current, and that such information is accessible in a timely way by competent authorities.

54 Countries are not required to give legal recognition to trusts. Countries need not include the requirements of Criteria 25.1; 25.2; 25.3; and 25.4 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

55 Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

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 co-operation 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[56].

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.

[56] This does not affect the requirements for proportionate and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

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[57], 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

[57] The Core Principles which are relevant to AML/CFT include: Basel Committee on Banking Supervision (BCBS) Principles 1-3, 5-9, 11-15, 26, and 29; International Association of Insurance Supervisors (IAIS) Principles 1, 3-11, 18, 21-23, and 25; and International Organization of Securities Commission (IOSCO) Principles 24, 28, 29 and 31; and Responsibilities A, B, C and D. Assessors may refer to existing assessments of the country's compliance with these Core Principles, where available.

(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 risk-based approach.

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[58] 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.

58 The supervisor's power to compel production of or to obtain access for supervisory purposes should not be predicated on the need to require a court order.

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 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 self-regulatory body (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 risk-based approach, when assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs.

RECOMMENDATION 29 FINANCIAL INTELLIGENCE UNITS (FIU)

29.1 Countries should establish an 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.[59]

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[60] 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:

---

59 Considering that there are different FIU models, Recommendation 29 does not prejudge a country's choice for a particular model, and applies equally to all of them.

60 This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate commercially held data.

(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 decision to analyse, request and/or forward or disseminate specific information;

(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[61], 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.

---

61 A '*parallel financial investigation*' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s).

A '*financial investigation*' means an enquiry into the financial affairs related to a criminal activity, with a view to: (i) identifying the extent of criminal networks and/or the scale of criminality; (ii) identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and (iii) developing evidence which can be used in criminal proceedings.

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

Note to Assessors:
Recommendation 32 may be implemented on a supra-national basis by a supra-national jurisdiction, such that only movements that cross the external borders of the supra-national jurisdiction are considered to be cross-border for the purposes of Recommendation 32. Such arrangements are assessed on a supra-national basis, on the basis set out in Annex I.

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[62] 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.

62 At a minimum, the information should set out (i) the amount of currency or BNIs declared, disclosed or otherwise detected, and (ii) the identification data of the bearer(s).

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) STRs, 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.[63]

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

[63] The sanctions should be directly or indirectly applicable for a failure to comply. They need not be in the same document that imposes or underpins the requirement, and can be in another document, provided there are clear links between the requirement and the available sanctions.

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[64] the Vienna Convention, the Palermo Convention, the Merida Convention and the Terrorist Financing Convention.

64 The relevant articles are: the Vienna Convention (Articles 3-11, 15, 17 and 19), the Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31, & 34), the Merida Convention (Articles 14-17, 23-24, 26-31, 38, 40, 43-44, 46, 48, 50-55, 57-58), and the Terrorist Financing Convention (Articles 2-18).

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 Recommendation 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 Recommendation31 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 co-operation 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[65] in place.

[65] Such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

RECOMMENDATION 40 OTHER FORMS OF INTERNATIONAL CO-OPERATION

General Principles

40.1 Countries should ensure that their competent authorities can rapidly provide the widest range of international co-operation 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 co-operation;

(b) be authorised to use the most efficient means to co-operate;

(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 co-operate, these should be negotiated and signed in a timely way, and with the widest range of foreign counterparts.

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

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

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

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

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

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

40.6 Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only for the purpose for, and by the authorities, for

which the information was sought or provided, unless prior authorisation has been given by the requested competent authority.

40.7 Competent authorities should maintain appropriate confidentiality for any request for co-operation 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 co-operation on money laundering, associated predicate offences and terrorist financing[66].

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[67]

40.12 Financial supervisors should have a legal basis for providing co-operation 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.

---

66 FIUs should be able to provide cooperation regardless of whether their counterpart FIU is administrative, law enforcement, judicial or other in nature.

67 This refers to financial supervisors which are competent authorities and does not include financial supervisors which are SRBs.

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

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

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

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

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

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

Exchange of information between law enforcement authorities

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

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

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

Exchange of information between non-counterparts

40.20 Countries should permit their competent authorities to exchange information indirectly[68] 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.

68 Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country.

EFFECTIVENESS ASSESSMENT

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.

Characteristics of an effective system

A country properly identifies, assesses and understands its money laundering and terrorist financing risks, and co-ordinates domestically to put in place actions to mitigate these risks. This includes the involvement of competent authorities and other relevant authorities; using a wide range of reliable information sources; using the assessment(s) of risks as a basis for developing and prioritising AML/CFT policies and activities; and communicating and implementing those policies and activities in a co-ordinated way across appropriate channels. The relevant competent authorities also co-operate, and co-ordinate policies and activities to combat the financing of proliferation. Over time, this results in substantial mitigation of money laundering and terrorist financing risks.

This outcome relates primarily to Recommendations 1, 2, 33 and 34.

Note to Assessors:

1) Assessors are not expected to conduct an in-depth review of, or assess the country's assessment(s) of risks. Assessors, based on their views of the reasonableness of the assessment(s) of risks, should focus on how well the competent authorities use their understanding of the risks in practice to inform policy development and actions to mitigate the risks.

2) Assessors should take into consideration their findings for this Immediate Outcome (IO) in their assessment of the other IOs. However, assessors should only let their findings relating to the co-operation and co-ordination of measures to combat the financing of proliferation affect the assessments of IO.11 and not of the other IOs. (*i.e.* IO.2 to IO.10) that deal with combating money laundering and terrorist financing.

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. 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?

a) Examples of Information that could support the conclusions on Core Issues

1. The country's assessment(s) of its ML/TF risks (e.g., *types of assessment(s) produced; types of assessment(s) published / communicated*).

2. AML/CFT policies and strategies (e.g., *AML/CFT policies, strategies and statements communicated/published; engagement and commitment at the senior officials and political level*).

3. Outreach activities to private sector and relevant authorities (e.g., *briefings and guidance on relevant conclusions from risk assessment(s); frequency and relevancy of consultation on policies and legislation, input to develop risk assessment(s) and other policy products*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

4. What are the methods, tools, and information used to develop, review and evaluate the conclusions of the assessment(s) of risks? How comprehensive are the information and data used?

5. How useful are strategic financial intelligence, analysis, typologies, and guidance?

6. Which competent authorities and relevant stakeholders (including financial institutions and DNFBPs) are involved in the assessment(s) of risks? How do they provide inputs to the national level ML/TF assessment(s) of risks, and at what stage?

7. Is the assessment(s) of risks kept up-to-date, reviewed regularly and responsive to significant events or developments (including new threats and trends)?

8. To what extent is the assessment(s) of risks reasonable and consistent with the ML/TF threats, vulnerabilities and specificities faced by the country? Where appropriate, does it take into account risks identified by other credible sources?

9. Do the policies of competent authorities respond to changing ML/TF risks?

10. What mechanism(s) or body do the authorities use to ensure proper and regular co-operation and co-ordination of the national framework and development and

implementation of policies to combat ML/TF, at both policymaking and operational levels, and where relevant, the financing of proliferation of weapons of mass destruction? Does the mechanism or body include all relevant authorities?

11. Are there adequate resources and expertise involved in conducting the assessment(s) of risks, and for domestic co-operation and co-ordination?

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

Characteristics of an effective system

The country provides constructive and timely information or assistance when requested by other countries. Competent authorities assist with requests to:

- locate and extradite criminals; and
- identify, freeze, seize, confiscate and share assets and provide information (including evidence, financial intelligence, supervisory and beneficial ownership information) related to money laundering, terrorist financing or associated predicate offences.

Competent authorities also seek international co-operation to pursue criminals and their assets. Over time, this makes the country an unattractive location for criminals (including terrorists) to operate in, maintain their illegal proceeds in, or use as a safe haven.

This outcome relates primarily to Recommendations 36 - 40 and also elements of Recommendations 9, 24, 25 and 32.

Note to Assessors:

Assessors should take into consideration how their findings on the specific role of relevant competent authorities in seeking and delivering international co-operation under this IO would impact other IOs (particularly IO.3, IO.5, IOs. 6 to 10) including how the country seeks international co-operation with respect to domestic cases when appropriate.

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 co-operation 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?

a) Examples of Information that could support the conclusions on Core Issues

1. Evidence of handling and making requests for international co-operation with respect to extradition, mutual legal assistance and other forms of international co-operation (*e.g., number of requests made, received, processed, granted, or refused relating to different competent authorities (e.g., central authority, FIU, supervisors, and law enforcement agencies) and types of request; timeliness of response, including prioritisation of requests; cases of spontaneous dissemination / exchange*).
2. Types and number of co-operation arrangements with other countries (including bilateral and multilateral MOUs, treaties, co-operation based on reciprocity, or other co-operation mechanisms).
3. Examples of: (a) making, and (b) providing successful international co-operation (e.g., *making use of financial intelligence / evidence provided to or by the country (as the case may be); investigations conducted on behalf or jointly with foreign counterparts; extradition of suspects/criminals for ML/TF*).
4. Information on investigations, prosecutions, confiscation and repatriation/sharing of assets (e.g., *number of ML/TF investigations/ prosecutions, number and value of assets frozen and confiscated (including non-conviction-based confiscation) arising from international co-operation; value of assets repatriated or shared*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

5. What operational measures are in place to ensure that appropriate safeguards are applied, requests are handled in a confidential manner to protect the integrity of the process (*e.g.,* investigations and inquiry), and information exchanged is used for authorised purposes?
6. What mechanisms (including case management systems) are used among the different competent authorities to receive, assess, prioritise and respond to requests for assistance?
7. What are the reasons for refusal in cases where assistance is not or cannot be provided?
8. What mechanisms (including case management systems) are used among the different competent authorities to select, prioritise and make requests for assistance?
9. How do different competent authorities ensure that relevant and accurate information is provided to the requested country to allow it to understand and assess the requests?

10. How well has the country worked with the requesting or requested country to avoid or resolve conflicts of jurisdiction or problems caused by poor quality information in requests?

11. How do competent authorities ensure that details of the contact persons and requirements for international co-operation requests are clear and easily available to requesting countries?

12. To what extent does the country prosecute its own nationals without undue delay in situations when it is unable by law to extradite them?

13. What measures and arrangements are in place to manage and repatriate assets confiscated at the request of other countries?

14. Are there aspects of the legal, operational or judicial process (*e.g.,* excessively strict application of dual criminality requirements etc.) that impede or hinder international co-operation?

15. To what extent are competent authorities exchanging information, indirectly, with non-counterparts?

16. Are adequate resources available for: (a) receiving, managing, coordinating and responding to incoming requests for co-operation; and (b) making and coordinating requests for assistance in a timely manner?

Immediate Outcome 3	Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks.

Characteristics of an effective system

Supervision and monitoring address and mitigate the money laundering and terrorist financing risks in the financial and other relevant sectors by:

- preventing criminals and their associates from holding, or being the beneficial owner of, a significant or controlling interest or a management function in financial institutions or DNFBPs; and
- promptly identifying, remedying, and sanctioning, where appropriate, violations of AML/CFT requirements or failings in money laundering and terrorist financing risk management.

Supervisors[69] provide financial institutions and DNFBPs with adequate feedback and guidance on compliance with AML/CFT requirements. Over time, supervision and monitoring improve the level of AML/CFT compliance, and discourage attempts by criminals to abuse the financial and DNFBP sectors, particularly in the sectors most exposed to money laundering and terrorist financing risks.

This outcome relates primarily to Recommendations 14, 26 to 28, 34 and 35, and also elements of Recommendations 1 and 40.

Note to Assessors:

Assessors should also consider the relevant findings, including at the financial group level, the level of international co-operation which supervisors are participating in when assessing this IO.

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?

[69] References to "Supervisors" include SRBs for the purpose of the effectiveness assessment.

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?

a) Examples of Information that could support the conclusions on Core Issues

1. Contextual factors regarding the size, composition, and structure of the financial and DNFBP sectors and informal or unregulated sector (e.g., *number and types of financial institutions (including MVTS) and DNFBPs licensed or registered in each category; types of financial (including cross-border) activities; relative size, importance and materiality of sectors*).

2. Supervisors' risk models, manuals and guidance on AML/CFT (e.g., *operations manuals for supervisory staff; publications outlining AML/CFT supervisory / monitoring approach; supervisory circulars, good and poor practises, thematic studies; annual reports*).

3. Information on supervisory engagement with the industry, the FIU and other competent authorities on AML/CFT issues (e.g., *providing guidance and training, organising meetings or promoting interactions with financial institutions and DNFBPs*).

4. Information on supervision (e.g., *frequency, scope and nature of monitoring and inspections (on-site and off-site); nature of breaches identified; sanctions and other remedial actions* (e.g., *corrective actions, reprimands, fines) applied, examples of cases where sanctions and other remedial actions have improved AML/CFT compliance*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

5. What are the measures implemented to prevent the establishment or continued operation of shell banks in the country?

6. To what extent are "fit and proper" tests or other similar measures used with regard to persons holding senior management functions, holding a significant or controlling interest, or professionally accredited in financial institutions and DNFBPs?

7. What measures do supervisors employ in order to assess the ML/TF risks of the sectors and entities they supervise/monitor? How often are the risk profiles reviewed, and what are the trigger events (e.g., changes in management or business activities)?

8. What measures and supervisory tools are employed to ensure that financial institutions (including financial groups) and DNFBPs are regulated and comply with their AML/CFT obligations (including those which relate to targeted financial sanctions on terrorism, and to

countermeasures called for by the FATF)? To what extent has this promoted the use of the formal financial system?

9. To what extent do the frequency, intensity and scope of on-site and off-site inspections relate to the risk profile of the financial institutions (including financial group) and DNFBPs?

10. What is the level of co-operation between supervisors and other competent authorities in relation to AML/CFT (including financial group ML/TF risk management) issues? What are the circumstances where supervisors share or seek information from other competent authorities with regard to AML/CFT issues (including market entry)?

11. What measures are taken to identify, license or register, monitor and sanction as appropriate, persons who carry out MVTs?

12. Do supervisors have adequate resources to conduct supervision or monitoring for AML/CFT purposes, taking into account the size, complexity and risk profiles of the sector supervised or monitored?

13. What are the measures implemented to ensure that financial supervisors have operational independence so that they are not subject to undue influence on AML/CFT matters?

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

Characteristics of an effective system

Financial institutions and DNFBPs understand the nature and level of their money laundering and terrorist financing risks; develop and apply AML/CFT policies (including group-wide policies), internal controls, and programmes to adequately mitigate those risks; apply appropriate CDD measures to identify and verify their customers (including the beneficial owners) and conduct ongoing monitoring; adequately detect and report suspicious transactions; and comply with other AML/CFT requirements. This ultimately leads to a reduction in money laundering and terrorist financing activity within these entities.

This outcome relates primarily to Recommendations 9 to 23, and also elements of Recommendations 1, 6 and 29.

Note to Assessors:

Assessors are not expected to conduct an in-depth review of the operations of financial institutions or DNFBPs, but should consider, on the basis of evidence and interviews with supervisors, FIUs, financial institutions and DNFBPs, whether financial institutions and DNFBPs have adequately assessed and understood their exposure to money laundering and terrorist financing risks; whether their policies, procedures and internal controls adequately address these risks; and whether regulatory requirements (including STR reporting) are being properly implemented.

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?

a) Examples of Information that could support the conclusions on Core Issues

1. Contextual factors regarding the size, composition, and structure of the financial and DNFBP sectors and informal or unregulated sector (e.g., *number and types of financial institutions (including MVTS) and DNFBPs licensed or registered in each category; types of financial (including cross-border) activities; relative size, importance and materiality of sectors*).
2. Information (including trends) relating to risks and general levels of compliance (e.g., *internal AML/CFT policies, procedures and programmes, trends and typologies reports*).
3. Examples of compliance failures (e.g., *sanitised cases; typologies on the misuse of financial institutions and DNFBPs*).
4. Information on compliance by financial institutions and DNFBPs (e.g., *frequency of internal AML/CFT compliance review; nature of breaches identified and remedial actions taken or sanctions applied; frequency and quality of AML/CFT training; time taken to provide competent authorities with accurate and complete CDD information for AML/CFT purposes; accounts/relationships rejected due to incomplete CDD information; wire transfers rejected due to insufficient requisite information*).
5. Information on STR reporting and other information as required by national legislation (e.g., *number of STRs submitted, and the value of associated transactions; number and proportion of STRs from different sectors; the types, nature and trends in STR filings corresponding to ML/TF risks; average time taken to analyse the suspicious transaction before filing an STR*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

6. What are the measures in place to identify and deal with higher (and where relevant, lower) risk customers, business relationships, transactions, products and countries?
7. Does the manner in which AML/CFT measures are applied prevent the legitimate use of the formal financial system, and what measures are taken to promote financial inclusion?
8. To what extent do the CDD and enhanced or specific measures vary according to ML/TF risks across different sectors / types of institution, and individual institutions? What is the relative level of compliance between international financial groups and domestic institutions?
9. To what extent is there reliance on third parties for the CDD process and how well are the controls applied?

10. How well do financial institutions and groups, and DNFBPs ensure adequate access to information by the AML/CFT compliance function?

11. Do internal policies and controls of the financial institutions and groups, and DNFBPs enable timely review of: (i) complex or unusual transactions, (ii) potential STRs for reporting to the FIU, and (iii) potential false-positives? To what extent do the STRs reported contain complete, accurate and adequate information relating to the suspicious transaction?

12. What are the measures and tools employed to assess risk, formulate and review policy responses and institute appropriate risk mitigation and systems and controls for ML/TF risks?

13. How are AML/CFT policies and controls communicated to senior management and staff? What remedial actions and sanctions are taken by financial institutions and DNFBPs when AML/CFT obligations are breached?

14. How well are financial institutions and DNFBPs documenting their ML/TF risk assessments, and keeping them up to date?

15. Do financial institutions and DNFBPs have adequate resources to implement AML/CFT policies and controls relative to their size, complexity, business activities and risk profile?

16. How well is feedback provided to assist financial institutions and DNFBPs in detecting and reporting suspicious transactions?

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.

Characteristics of an effective system:

Measures are in place to:

- prevent legal persons and arrangements from being used for criminal purposes;
- make legal persons and arrangements sufficiently transparent; and
- ensure that accurate and up-to-date basic and beneficial ownership information is available on a timely basis.

Basic information is available publicly, and beneficial ownership information is available to competent authorities. Persons who breach these measures are subject to effective, proportionate and dissuasive sanctions. This results in legal persons and arrangements being unattractive for criminals to misuse for money laundering and terrorist financing.

This outcome relates primarily to Recommendations 24 and 25, and also elements of Recommendations 1, 10, 37 and 40.

Note to Assessors:

Assessors should also consider the relevant findings in relation to the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent to which competent authorities seek and are able to provide the appropriate assistance in relation to identifying and exchanging information (including beneficial ownership information) for legal persons and arrangements.

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?

a) Examples of Information that could support conclusion on Core Issues

1. Contextual information on the types, forms and basic features of legal persons and arrangements in the jurisdiction.

2. Experiences of law enforcement and other relevant competent authorities (e.g., *level of sanctions imposed for breach of the information requirements; where and how basic and beneficial ownership information (including information on the settler, trustee(s), protector and beneficiaries) is obtained; information used in supporting investigation*).

3. Typologies and examples of the misuse of legal persons and arrangements (e.g., *frequency with which criminal investigations find evidence of the country's legal persons and arrangements being used for ML/TF; legal persons misused for illegal activities dismantled or struck-off).*

4. Sources of basic and beneficial ownership information (e.g., *types of public information available to financial institutions and DNFBPs; types of information held in the company registry or by the company*).

5. Information on the role played by "gatekeepers" (e.g., *company service providers, accountants, legal professionals*) in the formation and administration of legal persons and arrangements.

6. Other information (e.g., *information on existence of legal arrangements; responses (positive and negative) to requests for basic or beneficial ownership information received from other countries; information on the monitoring of quality of assistance*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

7. What are the measures taken to enhance the transparency of legal persons (including dealing with bearer shares and share warrants, and nominee shareholders and directors) and arrangements?

8. How do relevant authorities ensure that accurate and up-to-date basic and beneficial ownership information on legal persons is maintained? Is the presence and accuracy of information monitored, tested/certified or verified?

9. To what extent is the time taken for legal persons to register changes to the required basic and beneficial ownership information adequate to ensure that the information is accurate

and up to date? Where applicable, to what extent are similar changes in legal arrangements registered in a timely manner?

10. To what extent can financial institutions and DNFBPs obtain accurate and up-to-date basic and beneficial ownership information on legal persons and arrangements? What is the extent of information that trustees disclose to financial institutions and DNFBPs?

11. Do the relevant authorities have adequate resources to implement the measures adequately?

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

Characteristics of an effective system

A wide variety of financial intelligence and other relevant information is collected and used by competent authorities to investigate money laundering, associated predicate offences and terrorist financing. This delivers reliable, accurate, and up-to-date information; and the competent authorities have the resources and skills to use the information to conduct their analysis and financial investigations, to identify and trace the assets, and to develop operational analysis.

This outcome relates primarily to Recommendations 29 to 32 and also elements of Recommendations 1, 2, 4, 8, 9, 34 and 40.

Note to Assessors:

1) This outcome includes the work that the FIU does to analyse STRs and other data; and the use by competent authorities of FIU products, other types of financial intelligence and other relevant information[70].

2) Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent which FIUs and law enforcement agencies are able to, and do seek appropriate financial and law enforcement intelligence and other information from their foreign counterparts.

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?

[70] The sources include information derived from STRs, cross-border reports on currency and bearer negotiable movements, law enforcement intelligence; criminal records; supervisory and regulatory information; and information with company registries etc. Where applicable, it would also include reports on cash transactions, foreign currency transactions, wire transfers records, information from other government agencies including security agencies; tax authorities, asset registries, benefits agencies, NPOs authorities; and information which can be obtained through compulsory measures from financial institutions and DNFBPs including CDD information and transaction records, as well as information from open sources.

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?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences of law enforcement and other competent authorities (e.g., *types of financial intelligence and other information available; frequency with which they are used as investigative tools).*
2. Examples of the co-operation between FIUs and other competent authorities and use of financial intelligence (e.g., *statistics of financial intelligence disseminated/exchanged; cases where financial intelligence was used in investigation and prosecution of ML/TF and associated predicate offences, or in identifying and tracing assets*).
3. Information on STRs (e.g., *number of STRs/cases analysed; perception of quality of information disclosed in STRs; frequency with which competent authorities come across examples of unreported suspicious transactions; cases of tipping-off; see also Immediate Outcome 4 for information on STR reporting).*
4. Information on other financial intelligence and information *(*e.g., *number of currency and bearer negotiable instruments reports receive, and analysed; types of information that law enforcement and other competent authorities receive or obtain/access from other authorities, financial institutions and DNFBPs).*
5. Other documents (e.g., *guidance on the use and reporting of STRs and other financial intelligence; typologies produced using financial intelligence*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

6. How well does the FIU access and use additional information to analyse and add value to STRs? How does the FIU ensure the rigour of its analytical assessments?
7. How well do competent authorities make use of the information contained in STRs and other financial intelligence to develop operational analysis?
8. To what extent does the FIU incorporate feedback from competent authorities, typologies and operational experience into its functions?
9. What are the mechanisms implemented to ensure full and timely co-operation between competent authorities, and from financial institutions, DNFBPs and other reporting entities

to provide the relevant information? Are there any impediments to the access of information?

10. To what extent do the STRs reported contain complete, accurate and adequate information relating to the suspicious transaction?

11. To what extent do the relevant competent authorities review and engage (including outreach by the FIU) reporting entities to enhance financial intelligence reporting?

12. Do the relevant authorities have adequate resources (including IT tools for data mining and analysis of financial intelligence and to protect its confidentiality) to perform its functions?

13. What are the measures implemented to ensure that the FIU has operational independence so that it is not subject to undue influence on AML/CFT matters?

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

Characteristics of an effective system

Money laundering activities, and in particular major proceeds-generating offences, are investigated; offenders are successfully prosecuted; and the courts apply effective, proportionate and dissuasive sanctions to those convicted. This includes pursuing parallel financial investigations and cases where the associated predicate offences occur outside the country, and investigating and prosecuting stand-alone money laundering offences. The component parts of the systems (investigation, prosecution, conviction, and sanctions) are functioning coherently to mitigate the money laundering risks. Ultimately, the prospect of detection, conviction, and punishment dissuades potential criminals from carrying out proceeds generating crimes and money laundering.

This outcome relates primarily to Recommendations 3, 30 and 31, and also elements of Recommendations 1, 2, 32, 37, 39 and 40.

Note to Assessors:

Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent to which law enforcement agencies are seeking appropriate assistance from their foreign counterparts in cross-border money laundering cases.

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.

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences and examples of investigations, prosecutions and convictions*(* e.g., *examples of cases rejected due to insufficient investigative evidence; what are the significant or complex ML cases that the country has investigated and prosecuted; examples of successful cases against domestic and transnational organised crime; cases where other criminal sanctions or measures are pursued instead of ML convictions).*
2. Information on ML investigations, prosecutions and convictions (e.g., *number of investigations and prosecutions for ML activity; proportion of cases leading to prosecution or brought to court; number or proportion of ML convictions relating to third party laundering, stand-alone offence, self-laundering, and foreign predicate offences; types of predicate crimes involved; level of sanctions imposed for ML offences; sanctions imposed for ML compared with those for other predicate offences).*

b) Examples of Specific Factors that could support the conclusions on Core Issues

3. What are the measures taken to identify, initiate and prioritise ML cases (at least in relation to all major proceeds-generating offences) for investigation (*e.g.,* focus between small and larger or complex cases, between domestic and foreign predicates etc.)?
4. To what extent, and how quickly, can competent authorities obtain or access relevant financial intelligence and other information required for ML investigations?
5. To what extent are joint or cooperative investigations (including the use of multi-disciplinary investigative units) and other investigative techniques (*e.g.,* postponing or waiving the arrest or seizure of money for the purpose of identifying persons involved) used in major proceeds generating offences?
6. How are ML cases prepared for timely prosecution and trial?
7. In what circumstances are decisions made not to proceed with prosecutions where there is indicative evidence of a ML offence?
8. To what extent are ML prosecutions: (i) linked to the prosecution of the predicate offence (including foreign predicate offences), or (ii) prosecuted as an autonomous offence?
9. How do the relevant authorities, taking into account the legal systems, interact with each other throughout the life-cycle of a ML case, from the initiation of an investigation, through gathering of evidence, referral to prosecutors and the decision to go to trial?
10. Are there other aspects of the investigative, prosecutorial or judicial process that impede or hinder ML prosecutions and sanctions?
11. Do the competent authorities have adequate resources (including financial investigation tools) to manage their work or address the ML risks adequately?
12. Are dedicated staff/units in place to investigate ML? Where resources are shared, how are ML investigations prioritised?

Immediate Outcome 8	Proceeds and instrumentalities of crime are confiscated.

Characteristics of an effective system

Criminals are deprived (through timely use of provisional and confiscation measures) of the proceeds and instrumentalities of their crimes (both domestic and foreign) or of property of an equivalent value. Confiscation includes proceeds recovered through criminal, civil or administrative processes; confiscation arising from false cross-border disclosures or declarations; and restitution to victims (through court proceedings). The country manages seized or confiscated assets, and repatriates or shares confiscated assets with other countries. Ultimately, this makes crime unprofitable and reduces both predicate crimes and money laundering.

This outcome relates primarily to Recommendations 1, 4, 32 and also elements of Recommendations 30, 31, 37, 38, and 40.

Note to Assessors:

Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent which law enforcement and prosecutorial agencies are seeking appropriate assistance from their foreign counterparts in relation to cross-border proceeds and instrumentalities of crime.

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?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences and examples of confiscation proceedings (e.g., *the most significant cases in the past; types of confiscation orders obtained by the country; trends indicating changes in methods by which proceeds of crime is being laundered).*
2. Information on confiscation (e.g., *number of criminal cases where confiscation is pursued; type of cases which involve confiscation; value of proceeds of crimes, instrumentalities or property of equivalent value confiscated, broken down by foreign or domestic offences, whether through criminal or civil procedures (including non-conviction-based confiscation); value of falsely / not declared or disclosed cross-border currency and bearer negotiable instruments confiscated; value or proportion of seized or frozen proceeds that is subject to confiscation; value or proportion of confiscation orders realised*).
3. Other relevant information (*e.g. value of criminal assets seized / frozen*; *amount of proceeds of crime restituted to victims, shared or repatriated).*

b) Examples of Specific Factors that could support the conclusions on Core Issues

4. What are the measures and approach adopted by competent authorities to target proceeds and instrumentalities of crime (including major proceeds-generating crimes and those that do not originate domestically or have flowed overseas)?
5. How do authorities decide, at the outset of a criminal investigation, to commence a financial investigation, with a view to confiscation?
6. How well are competent authorities identifying and tracing proceeds and instrumentalities of crimes or assets of equivalent value? How well are provisional measures (*e.g.,* freeze or seizures) used to prevent the flight or dissipation of assets?
7. What is the approach adopted by the country to detect and confiscate cross-border currency and bearer negotiable instruments that are suspected to relate to ML/TF and associated predicate offences or that are falsely / not declared or disclosed?
8. What are the measures adopted to preserve and manage the value of seized/confiscated assets?
9. Are there other aspects of the investigative, prosecutorial or judicial process that promote or hinder the identification, tracing and confiscation of proceeds and instrumentalities of crime or assets of equivalent value?
10. Do the relevant competent authorities have adequate resources to perform their functions adequately?

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.

Characteristics of an effective system

Terrorist financing activities are investigated; offenders are successfully prosecuted; and courts apply effective, proportionate and dissuasive sanctions to those convicted. When appropriate, terrorist financing is pursued as a distinct criminal activity and financial investigations are conducted to support counter terrorism investigations, with good co-ordination between relevant authorities. The components of the system (investigation, prosecution, conviction and sanctions) are functioning coherently to mitigate the terrorist financing risks. Ultimately, the prospect of detection, conviction and punishment deters terrorist financing activities.

This outcome relates primarily to Recommendations 5, 30, 31 and 39, and also elements of Recommendations 1, 2, 32, 37 and 40.

Note to Assessors:

1) Assessors should be aware that some elements of this outcome may involve material of a sensitive nature (*e.g.,* information that is gathered for national security purposes) which countries may be reluctant or not able to make available to assessors.

2) Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome. This would involve considering the extent which law enforcement and prosecutorial agencies are seeking appropriate assistance from their foreign counterparts in cross-border terrorist financing cases.

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?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences and examples of TF investigations and prosecutions (e.g., *cases where TF investigations are used to support counter-terrorism investigations and prosecutions; significant cases where (foreign or domestic) terrorists and terrorist groups are targeted, prosecuted or disrupted; observed trends in TF levels and techniques; cases where other criminal sanctions or measures are pursued instead of TF convictions).*

2. Information on TF investigations, prosecutions and convictions (e.g., *number of TF investigations and prosecutions; proportion of cases leading to TF prosecution, type of TF prosecutions and convictions (*e.g., *distinct offences, foreign or domestic terrorists); level of sanctions imposed for TF offences; sanctions imposed for TF compared with those for other criminal activity; types and level of disruptive measures applied*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

3. What are the measures taken to identify, initiate and prioritise TF cases to ensure prompt investigation and action against major threats and to maximise disruption?

4. To what extent and how quickly can competent authorities obtain and access relevant financial intelligence and other information required for TF investigations and prosecutions?

5. What are the underlying considerations for decisions made not to proceed with prosecutions for a TF offence?

6. To what extent do the authorities apply specific action plans or strategies to deal with particular TF threats and trends? Is this consistent with the national AML/CFT policies, strategies and risks?

7. How well do law enforcement authorities, the FIU, counter-terrorism units and other security and intelligence agencies co-operate and co-ordinate their respective tasks associated with this outcome?

8. Are there other aspects of the investigative, prosecutorial or judicial process that impede or hinder TF prosecutions, sanctions or disruption?

9. Do the competent authorities have adequate resources (including financial investigation tools) to manage their work or address the TF risks adequately?

10. Are dedicated staff/units in place to investigate TF? Where resources are shared, how are TF investigations prioritised?

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

Characteristics of an effective system

Terrorists, terrorist organisations and terrorist support networks are identified and deprived of the resources and means to finance or support terrorist activities and organisations. This includes proper implementation of targeted financial sanctions against persons and entities designated by the United Nations Security Council and under applicable national or regional sanctions regimes. The country also has a good understanding of the terrorist financing risks and takes appropriate and proportionate actions to mitigate those risks, including measures that prevent the raising and moving of funds through entities or methods which are at greatest risk of being misused by terrorists. Ultimately, this reduces terrorist financing flows, which would prevent terrorist acts.

This outcome relates primarily to Recommendations 1, 4, 6 and 8, and also elements of Recommendations 14, 16, 30 to 32, 37, 38 and 40.

Note to Assessors:

Assessors should also consider the relevant findings on the level of international co-operation which competent authorities are participating in when assessing this Immediate Outcome.

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?

a) Examples of Information that could support the conclusions on Core Issues

1. Experiences of law enforcement, FIU and counter terrorism authorities (e.g., *trends indicating that terrorist financiers are researching alternative methods for raising /*

transmitting funds; intelligence/source reporting indicating that terrorist organisations are having difficulty raising funds in the country).

2. Examples of interventions and confiscation (e.g., *significant cases where terrorists, terrorist organisations or terrorist financiers are prevented from raising, moving and using funds or their assets seized / confiscated; investigations and interventions in NPOs misused by terrorists).*

3. Information on targeted financial sanctions (e.g., *persons and accounts subject to targeted financial sanctions under UNSC or other designations; designations made (relating to UNSCR1373); assets frozen; transactions rejected; time taken to designate individuals; time taken to implement asset freeze following designation*).

4. Information on NPO supervision and monitoring (*e.g. frequency of review and monitoring of the NPO sector (including risk assessments); frequency of engagement and outreach (including guidance) to NPO sector regarding CFT measures and trends; remedial measures and sanctions taken against NPOs*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

5. What measures has the country adopted to ensure the proper implementation of targeted financial sanctions without delay? How are those designations and obligations communicated to financial institutions, DNFBPs and the general public in a timely manner?

6. How well are the procedures and mechanisms implemented for (i) identifying targets for designation / listing, (ii) freezing / unfreezing, (iii) de-listing, and (iv) granting exemption? How well is the relevant information collected?

7. To what extent is the country utilising the tools provided by UNSCRs 1267 and 1373 to freeze and prevent the financial flows of terrorists?

8. How well do the systems for approving or licensing the use of assets by designated entities for authorised purposes comply with the requirements set out in the relevant UNSCRs (*e.g.,* UNSCR 1452 and any successor resolutions)?

9. What is the approach adopted by competent authorities to target terrorist assets? To what extent are assets tracing, financial investigations and provisional measures (*e.g.,* freezing and seizing) used to complement the approach?

10. What is the level of licensing or registration for NPOs? To what extent is a risk-sensitive approach taken to supervise or monitor NPOs at risk from terrorist abuse and appropriate preventive, investigative, criminal, civil or administrative actions and co-operation mechanisms adopted?

11. How well do NPOs understand their vulnerabilities and comply with the measures to protect themselves from the threat of terrorist abuse?

12. Are there other aspects of the investigative, prosecutorial or judicial process that promote or hinder the identification, tracing and deprivation of assets and instrumentalities related to terrorists, terrorist organisations or terrorist financiers?

13. Do the relevant competent authorities have adequate resources to manage their work or address the TF risks adequately

14. Where resources are shared, how are TF related activities prioritised?

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.

Characteristics of an effective system

Persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMD) are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation. Targeted financial sanctions are fully and properly implemented without delay; monitored for compliance and there is adequate co-operation and co-ordination between the relevant authorities to prevent sanctions from being evaded, and to develop and implement policies and activities to combat the financing of proliferation of WMD.

This outcome relates to Recommendation 7 and elements of Recommendation 2.

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?

a) Examples of Information that could support the conclusions on Core Issues

1. Examples of investigations and intervention relating to financing of proliferation (e.g., *investigations into breaches of sanctions; significant cases in which country has taken enforcement actions (*e.g., *freezing or seizures) or provided assistance).*

2. Information on targeted financial sanctions relating to financing of proliferation (e.g., *accounts of individuals and entities subject to targeted financial sanctions; value of frozen assets and property; time taken to designate persons and entities; time taken to freeze assets and property of individuals and entities following their designation by the UNSC*).

3. Monitoring and other relevant information relating to financing of proliferation (*e.g., frequency of review and monitoring of financial institutions and DNFBPs for compliance with targeted financial sanctions; frequency of engagement and outreach; guidance documents; level of sanctions applied on financial institutions and DNFBPs for breaches*).

b) Examples of Specific Factors that could support the conclusions on Core Issues

4. What measures has the country adopted to ensure the proper implementation of targeted financial sanctions relating to financing of proliferation without delay? How are these designations and obligations communicated to relevant sectors in a timely manner?

5. Where relevant, how well are the procedures implemented for (i) designation / listing, (ii) freezing / unfreezing, (iii) de-listing, and (iv) granting exemption? To what extent do they comply with the UNSCR requirements?

6. How well do the systems and mechanisms for managing frozen assets and licensing the use of assets by designated individuals and entities for authorised purposes, safeguard human rights and prevent the misuse of funds?

7. What mechanisms are used to prevent the evasion of sanctions? Do relevant competent authorities provide financial institutions and DNFBPs with other guidance or specific feedback?

8. To what extent would the relevant competent authorities be able to obtain accurate basic and beneficial ownership information on legal persons (*e.g.,* front companies), when investigating offences or breaches concerning the UNSCRs relating financing of proliferation?

9. To what extent are the relevant competent authorities exchanging intelligence and other information for investigations of violations and breaches of targeted financial sanctions in relation to financing of proliferation, as per the relevant UNSCRs?

10. Do the relevant competent authorities have adequate resources to manage their work or address the financing of proliferation risks adequately?

ANNEX I:

SUPRA-NATIONAL ASSESSMENT

[Annex to be finalised]

ANNEX II

MUTUAL EVALUATION REPORT TEMPLATE

[Annex to be finalised]

FATF GUIDANCE DOCUMENTS

Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons (June 1998).

Guidance for Financial Institutions in Detecting Terrorist Financing (April 2002).

International Best Practices: Combating the Abuse of Non-Profit Organisations (October 2002).

International Best Practices: Combating the Abuse of Alternative Remittance Systems (June 2003).

The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction (June 2007).

Guidance on the Risk-Based Approach (June 2007 - October 2009) for:

- the Financial Sector;
- Real Estate Agents;
- Accountants;
- TCSPs;
- Dealers in precious metals and stones;
- Casinos;
- Legal Professionals;
- Money Service Businesses; and
- the Life Insurance Sector.

The Implementation of Activity-Based Financial Prohibitions of United Nations Security Council Resolution 1737 (October 2007).

Capacity Building for Mutual Evaluations and Implementation of the FATF Standards within Low Capacity Countries (February 2008).

Best Practices Paper on Trade Based Money Laundering (June 2008).

The Implementation of Financial Provisions of UN Security Council Resolution 1803 (October 2008).

International Best Practices: Freezing of Terrorist Assets (June 2009).

International Best Practices: Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments (February 2010).

Best Practices Paper on Recommendation 2: Sharing among domestic competent authorities information related to the financing of proliferation (March 2012)

Financial Investigations Guidance (July 2012)

Best Practices: Managing the anti-money laundering and counter-terrorist financing policy implications of voluntary tax compliance programmes (October 2012)

Best Practices on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery (October 2012)

FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion (February 2013)

Guidance on National Money Laundering / Terrorist Financing Risk Assessment (February 2013)

LEGAL BASIS OF REQUIREMENTS ON FINANCIAL INSTITUTIONS AND DNFBPS

1. All requirements for financial institutions or DNFBPs should be introduced either (a) in law (see the specific requirements in Recommendations 10, 11 and 20 in this regard), or (b) for all other cases, in law or enforceable means (the country has discretion).

2. In Recommendations 10, 11 and 20, the term "*law*" refers to any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.

3. The term "*Enforceable means*" refers to regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35).

4. In considering whether a document or mechanism has requirements that amount to *enforceable means*, the following factors should be taken into account:

   (a) There must be a document or mechanism that sets out or underpins requirements addressing the issues in the FATF Recommendations, and providing clearly stated requirements which are understood as such. For example:

      (i) if particular measures use the word *shall* or *must*, this should be considered mandatory;

      (ii) if they use *should*, this could be mandatory if both the regulator and the regulated institutions demonstrate that the actions are directly or indirectly required and are being implemented; language such as measures *are encouraged*, *are recommended* or institutions *should consider* is less likely to be regarded as mandatory. In any case where weaker language is used, there is a presumption that the language is not mandatory (unless the country can demonstrate otherwise).

   (b) The document/mechanism must be issued or approved by a competent authority.

   (c) There must be sanctions for non-compliance (sanctions need not be in the same document that imposes or underpins the requirement, and can be in another document, provided that there are clear links between the requirement and the

available sanctions), which should be effective, proportionate and dissuasive. This involves consideration of the following issues:

(i) there should be an adequate range of effective, proportionate and dissuasive sanctions available if persons fail to comply with their obligations;

(ii) the sanctions should be directly or indirectly applicable for a failure to comply with an AML/CFT requirement. If non-compliance with an AML/CFT requirement does not have a sanction directly attached to it, then the use of sanctions for violation of broader requirements, such as not having proper systems and controls or not operating in a safe and sound manner, is satisfactory provided that, at a minimum, a failure to meet one or more AML/CFT requirements could be (and has been as appropriate) adequately sanctioned without a need to prove additional prudential failures unrelated to AML/CFT; and

(iii) whether there is satisfactory evidence that effective, proportionate and dissuasive sanctions have been applied in practice.

5. In all cases it should be apparent that financial institutions and DNFBPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

GLOSSARY

Terms	Definitions
Accounts	References to "accounts" should be read as including other similar business relationships between financial institutions and their customers.
Accurate	Is used to describe information that has been verified for accuracy.
Agent	For the purposes of Recommendations 14 and 16, agent means any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.
Appropriate authorities	Refers to competent authorities, including accrediting institutions, and self-regulatory organisations.
Associate NPOs	Includes foreign branches of international NPOs.
Batch transfer	Is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Bearer negotiable instruments	*Bearer negotiable instruments (BNIs)* includes monetary instruments in bearer form such as: traveller's cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.
Bearer shares	*Bearer shares* refers to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.
Beneficial owner	*Beneficial owner* refers to the natural person(s) who ultimately[71] owns or controls a customer[72] and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiary	The meaning of the term *beneficiary* in the FATF Recommendations depends on the context:

71 Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

72 This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

Terms	Definitions
	■ In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. ■ In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy. It also refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO. Refers as well to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.
Beneficiary Financial Institution	Refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.
Competent authorities	*Competent authorities* refers to all public authorities[73] with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.
Confiscation	The term *confiscation,* which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or

[73] This includes financial supervisors established as independent non-governmental authorities with statutory powers.

Terms	Definitions
	administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State[74]. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.
Core Principles	*Core Principles* refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Correspondent banking	*Correspondent banking* is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (*e.g.,* interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
Country	All references in the FATF Recommendations to *country* or *countries* apply equally to territories or jurisdictions.
Cover Payment	Refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
Criminal activity	*Criminal activity* refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3.
Cross-border Wire Transfer	Refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of *wire transfer* in which at least one of the financial institutions involved is located in a different country.
Currency	*Currency* refers to banknotes and coins that are in circulation as a medium of exchange.

[74] For the purposes of the effectiveness assessment, "confiscation" may have a wider application.

Terms	Definitions
Designated categories of offences	*Designated categories of offences* means: ■ participation in an organised criminal group and racketeering; ■ terrorism, including terrorist financing; ■ trafficking in human beings and migrant smuggling; ■ sexual exploitation, including sexual exploitation of children; ■ illicit trafficking in narcotic drugs and psychotropic substances; ■ illicit arms trafficking; ■ illicit trafficking in stolen and other goods; ■ corruption and bribery; ■ fraud; ■ counterfeiting currency; ■ counterfeiting and piracy of products; ■ environmental crime; ■ murder, grievous bodily injury; ■ kidnapping, illegal restraint and hostage-taking; ■ robbery or theft; ■ smuggling; (including in relation to customs and excise duties and taxes); ■ tax crimes (related to direct taxes and indirect taxes); ■ extortion; ■ forgery; ■ piracy; and ■ insider trading and market manipulation. When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.
Designated non-financial businesses and professions	*Designated non-financial businesses and professions* means: a) Casinos[75] b) Real estate agents.

[75] References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

Terms	Definitions
	c) Dealers in precious metals. d) Dealers in precious stones. e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures. f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: ■ acting as a formation agent of legal persons; ■ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; ■ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; ■ acting as (or arranging for another person to act as) a trustee of an express trust 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.
Designated person or entity	The term *designated person or entity* refers to: (i) individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida; (ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; (iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001); (iv) any natural or legal person or entity designated for the application of

Terms	Definitions
	targeted financial sanctions pursuant to Security Council resolution 1718 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the *"Security Council Committee established pursuant to resolution 1718 (2006)"* (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and (v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1737 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the *"Security Council Committee established pursuant to paragraph 18 of resolution 1737 (2006)"* (the 1737 Sanctions Committee) pursuant to resolution 1737 (2006) and its successor resolutions.
Designation	The term *designation* refers to the identification of a person[76] or entity that is subject to targeted financial sanctions pursuant to: ■ United Nations Security Council resolution 1267 (1999) and its successor resolutions; ■ Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination; ■ Security Council resolution1718 (2006) and its successor resolutions; ■ Security Council resolution 1737 (2006) and its successor resolutions; and ■ any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction.
Domestic Wire Transfer	Refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of *wire transfer* that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country. The term also refers to any chain of *wire transfer* that takes place entirely within the borders of the European Economic Area (EEA)[77].
Enforceable	The term "*Enforceable means*" refers to regulations, guidelines, instructions or

76 Natural or legal.

77 An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of Recommendation 16 compliance.

Terms	Definitions
means	other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35).
Ex Parte	The term *ex parte* means proceeding without prior notification and participation of the affected party.
Express trust	*Express trust* refers to a trust clearly created by the settlor, usually in the form of a document *e.g.,* a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (*e.g.,* constructive trust).
False declaration	Refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	Refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.
Financial group	*Financial group* means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Financial institutions	*Financial institutions* means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public.[78] 2. Lending.[79] 3. Financial leasing.[80] 4. Money or value transfer services.[81]

78 This also captures private banking.

79 This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

80 This does not extend to financial leasing arrangements in relation to consumer products.

81 It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.

Terms	Definitions
	5. Issuing and managing means of payment (*e.g.,* credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 7. Trading in: (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading. 8. Participation in securities issues and the provision of financial services related to such issues. 9. Individual and collective portfolio management. 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. 11. Otherwise investing, administering or managing funds or money on behalf of other persons. 12. Underwriting and placement of life insurance and other investment related insurance[82]. 13. Money and currency changing.
Foreign counterparts	Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the co-operation which is sought, even where such foreign competent authorities have a different nature or status (*e.g.,* depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).
Freeze	In the context of confiscation and provisional measures (*e.g.,* Recommendations 4, 32 and 38), the term freeze means to prohibit the transfer, conversion, disposition or movement of any property, equipment or other instrumentalities on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism, or until a forfeiture or confiscation determination is made by a competent authority. For the purposes of Recommendations 6 and 7 on the implementation of targeted financial sanctions, the term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security

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

Terms	Definitions
	Council or in accordance with applicable Security Council resolutions by a competent authority or a court. In all cases, the frozen property, equipment, instrumentalities, funds or other assets remain the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such natural or legal person(s) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of a freeze, countries may decide to take control of the property, equipment, instrumentalities, or funds or other assets as a means to protect against flight.
Fundamental principles of domestic law	This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.
Funds	The term *funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.
Funds or other assets	The term *funds or other assets* means any assets, including, but not limited to, financial assets, economic resources, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.
Identification data	The term *identification data* refers to reliable, independent source documents, data or information.
Intermediary financial institution	Refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
International organisations	International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they

Terms	Definitions
	are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.
Law	In Recommendations 10, 11 and 20, the term "*law*" refers to any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.
Legal arrangements	*Legal arrangements* refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.
Legal persons	*Legal persons* refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.
Money laundering offence	References (except in Recommendation 3) to a *money laundering offence* refer not only to the primary offence or offences, but also to ancillary offences.
Money or value transfer service	*Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*.
Non-conviction based confiscation	*Non-conviction based confiscation* means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required.
Non-profit organisations	Refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of

Terms	Definitions
	"good works".
Ordering financial institution	Refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for an wire transfer on behalf of the originator.
Originator	Refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
Payable-through accounts	Refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.
Physical cross-border transportation	Refers to any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency or BNIs through containerised cargo or (3) the mailing of currency or BNIs by a natural or legal person.
Politically Exposed Persons (PEPs)	*Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Persons who are or have been entrusted with a prominent function by an international organisation* refers to members of senior management, *i.e.* directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Proceeds	*Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	*Property* means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Qualifying wire transfers	Means a cross-border wire transfer above any applicable threshold as described in paragraph 5 of the Interpretive Note to Recommendation 16 as follows: "Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:

Terms	Definitions
	(a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer. (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information."
Reasonable measures	The term *Reasonable Measures* means: appropriate measures which are commensurate with the money laundering or terrorist financing risks.
Related to terrorist financing or money laundering	When used to describe currency or BNIs, refers to currency or BNIs that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.
Required	Is used to describe a situation in which all elements of required information are present. Subparagraphs 6(a), 6(b) and 6(c) set out the *required originator information.* Subparagraphs 6(d) and 6(e) set out the *required beneficiary information*.
Risk	All references to *risk* refer to the risk of money laundering and/or terrorist financing. This term should be read in conjunction with the Interpretive Note to Recommendation 1.
Satisfied	Where reference is made to a financial institution being *satisfied* as to a matter, that institution must be able to justify its assessment to competent authorities.
Seize	The term *seize* means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.
Self-regulatory body (SRB)	A SRB is a body that represents a profession (*e.g.,* lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to

Terms	Definitions
	ensure that high ethical and moral standards are maintained by those practising the profession.
Serial Payment	Refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (*e.g.,* correspondent banks).
Settlor	*Settlors* are natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.
Shell bank	*Shell bank* means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
Should	For the purposes of assessing compliance with the FATF Recommendations, the word *should* has the same meaning as *must.*
Straight-through processing	Refers to payment transactions that are conducted electronically without the need for manual intervention.
Supervisors	*Supervisors* refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("*financial supervisors*" [83]) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs[84]) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.
Targeted financial sanctions	The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
Terrorist	The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist

83 Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

84 For the purposes of the effectiveness assessment, "supervisors" includes SRBs.

Terms	Definitions
	act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist act	A *terrorist act* includes: (a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999). (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist financing	*Terrorist financing* is the financing of terrorist acts, and of terrorists and terrorist organisations.
Terrorist financing offence	References (except in Recommendation 4) to a *terrorist financing offence* refer not only to the primary offence or offences, but also to ancillary offences.
Terrorist organisation	The term *terrorist organisation* refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third parties	For the purposes of Recommendations 6 and 7, the term *third parties* includes, but is not limited to, financial institutions and DNFBPs. The term *third parties* means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17.

Terms	Definitions
Trustee	The terms *trust* and *trustee* should be understood as described in and consistent with Article 2 of the *Hague Convention on the law applicable to trusts and their recognition*[85]. Trustees may be professional (*e.g.,* depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non-professional (*e.g.,* a person acting without reward on behalf of family).
Unique transaction reference number	Refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
Without delay	The phrase *without delay* means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (*e.g.,* the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee or the 1737 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase *without delay* means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase *without delay* should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

85 Article 2 of the Hague Convention reads as follows:

For the purposes of this Convention, the term "trust" refers to the legal relationships created – inter-vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose.

A trust has the following characteristics -

a) the assets constitute a separate fund and are not a part of the trustee's own estate;

b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee;

c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.

The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

FATF

FATF GUIDANCE

National Money Laundering and Terrorist Financing Risk Assessment

February 2013

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

Table of Contents

ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIU	Financial Intelligence Units
INR. X	Interpretive Note to Recommendation X
ML	Money Laundering
NPO	Non-Profit Organisation
RBA	Risk-Based Approach
SRB	Self-Regulating Body
STR	Suspicious Transaction Report
TF	Terrorist Financing

1. INTRODUCTION & TERMINOLOGY

1.1 Purpose, scope and status of this guidance

1. Identifying, assessing, and understanding ML/TF risks is an essential part of the implementation and development of a national anti-money laundering / countering the financing of terrorism (AML/CFT) regime, which includes laws, regulations, enforcement and other measures to mitigate ML/TF risks. It assists in the prioritisation and efficient allocation of resources by authorities. The results of a national risk assessment, whatever its scope, can also provide useful information to financial institutions and designated non-financial businesses and professions (DNFBPs) to support the conduct of their own risk assessments. Once ML/TF risks are properly understood, country authorities may apply AML/CFT measures in a way that ensures they are commensurate with those risks – *i.e,.* the risk-based approach (RBA) – which is central to the FATF standards as is set out in Recommendation 1, its interpretive note (INR 1), as well as in other Recommendations (*e.g.,* Recommendations 10, 26 and 28).

2. This document is intended to provide guidance on the conduct of risk assessment at the country or national level, and it relates especially to key requirements set out in Recommendation 1 and paragraphs 3-6 of INR 1. In particular, it outlines general principles that may serve as a useful framework in assessing ML/TF risks at the national level. The guidance contained in this document takes into consideration previous FATF work[1], which is still valid reference material. The general principles contained in this paper are also relevant when conducting risk assessments of a more focussed scope, such as in assessments of a particular financial or DNFBP sector (for example, the securities sector) or of thematic issues (for example, the proceeds of corruption related ML). All of these types of assessments (comprehensive, sectoral or thematic) carried out at the national level may also form the basis for determining whether to apply enhanced or specific measures, simplified measures, or exemptions from AML/CFT requirements. Furthermore, while FATF Recommendation 1 does not create specific risk assessment obligations regarding the financing of proliferation of weapons of mass destruction, the general principles laid out in this guidance could also be used in conducting a risk assessment for this area.

3. The guidance in this document is not intended to explain how supervisors should assess risks in the context of risk-based supervision, although risk-based supervision will likely be informed by a national-level risk assessment. Also, this guidance does not provide further explanation of RBA obligations and decisions for financial institutions and DNFBPs. The FATF has issued separate

[1] See bibliography for a list of relevant FATF work, national-level assessments available online and other relevant material. Annex III contains summaries of selected country-level assessment processes.

guidance on implementing the RBA for specific sectors and professions[2], and that material will be reviewed and, as necessary, modified in light of the revised FATF Recommendations.

This guidance document is not a standard and is therefore not intended to designate specific actions necessary to meet obligations under Recommendation 1 and INR 1 or any other Recommendations dealing with the RBA. Criteria for technical compliance and for assessing effectiveness relevant to this and all other FATF Recommendations may be found in the FATF assessment methodology. The practices described in this guidance are intended to serve as examples that may facilitate implementation of these obligations in a manner compatible with the FATF standards.

4. This guidance is structured as follows:

- This section (1) lays out the purpose, scope and status of this guidance, along with an outline of the core FATF obligations relevant to ML/TF risk assessments at any level.
- Section 2 lays out general principles that should be taken into account when conducting ML/TF risk assessments at the country or national level.
- Section 3 discusses how to organise a national-level ML/TF risk assessment, its frequency, and the data and information that could be used while undertaking such an assessment.
- Section 4 presents a high-level view of the three main stages involved in the ML/TF risk assessment process (identification, analysis and evaluation).
- Section 5 considers the outcome and dissemination of the risk assessment product.
- Annexes to this document contain additional information relating to ML/TF risk assessment including summaries of selected national-level assessments.

1.2 Core FATF obligations and decisions regarding ML/TF risk assessments

5. It is important that the users of this guidance have an understanding of the obligations contained in Recommendation 1 and its interpretive note. This section provides a general outline of these obligations. For more details, reference should be made to the texts of Recommendation 1 and its interpretive note, as well as the FATF assessment methodology.[3]

6. **Recommendation 1:** The text of Recommendation 1 lays out a number of basic principles with regard to risk assessment. First, it calls on countries to "identify, assess and understand" the ML/TF risks they face, and states that countries should also designate "an authority or mechanism to co-ordinate actions to assess risks". The goal of the standard is to ensure that countries can

[2] Nine sectoral RBA guidance papers are available from the FATF website: www.fatf-gafi.org/. This guidance will be revised following adoption of the revised FATF Recommendations in February 2012.

[3] See FATF website (www.fatf-gafi.org) for these texts.

mitigate their ML/TF risks effectively, and the risk assessment is clearly intended to serve as the basis for application of the risk-based approach, *i.e.*, "to ensure that measures … are commensurate with the risks identified." The text of the Recommendation adds that the "[risk-based] approach" (and therefore the risk assessment process on which it is based) should also be "an essential foundation" in allocating AML/CFT resources efficiently. Furthermore, the Recommendation indicates that risk assessments carried out by countries should be used for determining higher and lower risks that may then be addressed by applying enhanced measures or allowing simplified measures respectively. The Recommendation concludes by requiring that financial institutions and DNFBPs should also be able to identify, assess and take effective action to mitigate ML/TF risks.

7. **Interpretive Note to Recommendation 1:** INR 1 provides more details on the requirement for countries to assess their ML/TF risks and on the purposes for which such assessments may be used[4]. In particular, it emphasises that the objective of the risk-based approach is to ensure AML/CFT measures are commensurate with the "risks identified", as well as to enable decision making on effective resource allocation. In elaborating on the specific obligations and decisions for countries, INR 1 states that countries should take steps to identify and assess their ML/TF risks on an "ongoing basis." The objectives of the process at the country level are: (1) to provide input for potential improvements to the AML/CFT regime, including through the formulation or calibration of national AML/CFT policies, (2) to help in prioritising and allocating AML/CFT resources by competent authorities, including through feeding into any risk assessments conducted by such competent authorities (*e.g.*, supervisors) and (3) to feed into the AML/CFT risk assessments carried out by financial institutions and DNFBPs. The text of the interpretive note indicates that supervisors, in accordance with Recommendations 26 and 28, should review the risk assessments prepared by financial institutions and DNFBPs and take the result of that review into consideration in their supervision. The text of INR. 1 also adds that country-level risk assessments should be kept up-to-date, and appropriate information should be shared with all relevant competent authorities, self-regulatory bodies, financial institutions and DNFBPs.

8. In the cases of higher and lower risk determination, country-level risk assessments have very specific roles: Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these risks. Where countries identify lower risks they may decide to allow simplified measures to be applied in relation to some of the FATF Recommendations.

1.3 Key concepts and terms relevant to ML/TF risk assessment

9. In discussing ML/TF risk assessment, it is useful to have a common understanding of certain key concepts and terms that will be used in this guidance. Many of these come from the area of *risk management*, a process commonly used in the public as well as the private sectors to help in decision-making. While many risk management concepts are usefully described elsewhere[5], their

[4] Footnote 1 of INR. 1 specifically acknowledges that supra-national risk assessments should be taken into account, where appropriate. It should be noted therefore that the general principles set out in this document that apply to risk assessments carried out by countries at a national level may also be appropriate to risk assessments carried out at a supra-national level. See Section 2 for further discussion of this issue.

[5] See for example (2009a), ISO (2009b) and ISO (2009c) [see bibliography].

use in this guidance has been adapted to the particular case of assessing ML/TF risk at the national level. Broadly speaking, however, risk management involves developing the appropriate measures to mitigate or reduce an assessed level of risk to a lower or acceptable level.

10. For the purposes of assessing ML/TF risk at the national level, this guidance uses the following key concepts:

- ***Risk*** can be seen as a function of three factors: *threat*, *vulnerability* and *consequence*. An ML/TF *risk assessment* is a product or process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand ML/TF risks and serves as a first step in addressing them. Ideally, a risk assessment, involves making judgments about threats, vulnerabilities and consequences, which are discussed below.
- A ***threat*** is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities. *Threat* is described above as one of the factors related to risk, and typically it serves as an essential starting point in developing an understanding of ML/TF risk. For this reason, having an understanding of the environment in which predicate offences are committed and the proceeds of crime are generated to identify their nature (and if possible the size or volume) is important in order to carry out an ML/TF risk assessment. In some instances, certain types of threat assessments might serve as a precursor for a ML/TF risk assessment.[6]
- The concept of ***vulnerabilities*** as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at *vulnerabilities* as distinct from *threat* means focussing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes.
- ***Consequence*** refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML or TF may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector. As stated above, ideally a risk assessment involves making judgments about threats, vulnerabilities

6 The United Nations Office on Drugs and Crime (UNODC) has published *Guidance on the preparation and use of serious and organised crime threat assessments* ("The SOCTA Handbook"), which provides useful information on the conduct of national threat assessments related to serious and organised crime.

and consequences. Given the challenges in determining or estimating the consequences of ML and TF it is accepted that incorporating consequence into risk assessments may not involve particularly sophisticated approaches, and that countries may instead opt to focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities. The key is that the risk assessment adopts an approach that attempts to distinguish the extent of different risks to assist with prioritising mitigation efforts.

1.4 Users of ML/TF risk assessments

11. The form, scope and nature of ML/TF risk assessments should ultimately meet the needs of its users – whether these are policy makers, supervisors, operational agencies, financial institutions, DNFBPs, etc. The number and diversity of users of an assessment varies according to the purpose for which it is carried out; however, typical users of risk assessments might include:

- Policy makers and other authorities, for example, in order to formulate the national AML/CFT policies, make reasonable decisions on the legal and regulatory framework and the allocation of resources to competent authorities on the basis of FATF Recommendation 2.
- Operational agencies, including law enforcement, other investigative authorities, financial intelligence units (FIUs), relevant border agencies, etc.
- Regulators, supervisors and self-regulatory bodies (SRBs).
- Financial institutions, and designated non-financial businesses and professions (DNFBPs), for which the national-level ML/TF risk assessment is a critical source[7] contributing to their own ML/TF risk assessments and risk-based obligations.
- Non-profit organisations (NPOs).
- AML/CFT assessors and assessment bodies more broadly, along with other international stakeholders.
- The general public, as well as academia, specified individuals, etc.

[7] According to the FATF standard, countries are expected to make appropriate information on the results of their national risk assessment available to financial institutions and DNFBPs for this purpose.

2. GENERAL PRINCIPLES FOR NATIONAL ML/TF RISK ASSESSMENTS

12. The general principles set out below could be considered when a country intends to conduct any kind of ML/TF risk assessment. These include considerations on the purpose and scope of the assessment as well as the process through which an assessment will be conducted; the stages of a risk assessment, the participants, users and other parties involved; the information which may be used, and the final outcome of the assessment process.

13. The nature, methodology, participants, and information required for an assessment depend on the purpose and scope of the assessment. There is no single or universal methodology for conducting an ML/TF risk assessment. Therefore, this guidance does not advocate the use of any particular methodology or process. This guidance is aimed to provide a generic description of the risk assessment process as it might be applied to looking at risk associated with ML/TF and considerations and practical tools for countries to take into account when undertaking their own ML/TF risk assessment.[8]

2.1 Clear agreement on purpose

14. Before starting any kind of ML/TF risk assessment, all parties involved, including those who will conduct the assessment and, as appropriate, the eventual end users should be in agreement on the purpose and scope of the assessment. Expectations should also be set as to how the results relate to the understanding of national-level risks. Generally, a ML/TF risk assessments is intended to help a country to identify, assess and ultimately understand the ML/TF risks it faces. A country may set out more concrete goals for a particular risk assessment however, such as informing the development of policy or the deployment of resources by supervisors, law enforcement and other competent authorities. Understanding the scale and impact of identified risks can also assist in determining the appropriate level and nature of AML/CFT controls applied to a particular product or sector. Given the diversity of potential users and possible diverging expectations, it is essential at the outset that there be clarity about why an assessment is to be conducted, the questions it should answer, the criteria that will be used to answer those questions and the possible decisions that the assessment will feed into.

15. ML/TF risk assessments may be tied to strategic planning and linked to specific actions or decisions. For example, a national ML/TF risk assessment serves as input to a national AML/CFT strategy or policy as part of the country's domestic AML/CFT co-ordination process. The purposes of the assessment will also vary according to the needs of the users. The purpose and scope of the assessment may also determine the methodology that is to be used.

[8] Nonetheless, those involved carrying out a national ML/TF risk assessment may gain further insight into risk concepts, methodologies, processes, and tools from consulting any requirements of their own government relating to risk assessment or other material on risk management standards and associated publications (see the bibliography at the end of this document for a list of some of these sources).

2.2 Determining scope

Money laundering and terrorist financing

16. A key consideration when deciding on the scope of an ML/TF risk assessment is to determine whether ML and TF risks should be assessed separately or together. Factors associated with TF that might need to be considered may be very different from those associated with ML. For example, funds used for financing of terrorist activities may be derived from criminal activity or legal sources. In addition, a key focus in combating TF is on preventing future terrorist acts from occurring whereas with combating ML, the criminal activity (the predicate offence) has already taken place. Another difference is that, transactions associated with TF may be conducted in very small amounts, which when not viewed in the TF context could be the very transactions that are frequently considered to involve minimal ML risk. Countries may therefore choose to assess their ML and TF risks separately.[9]

National, supranational and sub-national risk assessments

17. As stated throughout this guidance, ML/TF risk assessments may be undertaken at different levels and with differing purposes and scope, including supranational assessments (of a group of countries), national (or country level) assessments and sub-national assessments (of a particular sector, region, or operational function within a country) even though the basic obligation of assessing and understanding ML/TF risk rests on the country itself. In order to be of use in assessing and understanding national-level risks, it is helpful that assessments carried out at other levels relate to each other in a consistent way, although it is recognised that this may not be possible in all instances due to specific risks and the specific assessment approach undertaken. For example, the interplay between a national ML/TF assessment and specific sectoral ML/TF risk assessments could be considered as follows:

- High or low risk situations identified by the competent authorities through national ML/TF assessment should logically influence and/or confirm choices of higher, lower, or low risk situations relevant to the risk-based approach as implemented by financial institutions and DNFBPs, and overseen by supervisors or SRBs.
- Continuing examination by financial institutions and DNFBPs of their risks (regarding types of customers, products, etc.) as monitored by supervisory agencies would potentially contribute to and/or confirm identification of risk levels in the context of national ML/TF assessments.

18. In principle, a national ML/TF risk assessment can be composed of different types of assessments, and the different levels could be combined together to form a national-level understanding of the risk with each limited-scope assessment contributing to the overall picture. It may, for example, be possible for those conducting the ML/TF assessment to rely on a variety of assessments (for example, assessments conducted by supervisors and SRBs on the ML/TF risks in

[9] For the purposes of ML/TF risk assessment, this guidance discusses indicators or elements relating to ML and TF in Section 4 under the explanations of identification and analysis. Further relevant lists are provided in Annexes I and II.

financial and DNFBPs sectors, ML/TF risk assessments conducted by the firms operating in the financial and DNFBP sectors, threat assessments conducted by law enforcement agencies and FIUs on ML[10] and TF, assessments of the ML/TF vulnerabilities in the NPO sectors or legal persons and arrangements, and any ML/TF assessments carried out at the state level in a federation) to form a national-level understanding of the ML/TF risk.

19. The approach adopted by each country may also be dependent on the country's framework for co-ordinating and co-operating on AML/CFT matters. For example, in some cases, it might be more appropriate to pull together all or many of the relevant contributors to conduct a single national ML/TF risk assessment. This would also simplify the need to collate and compare different types of assessments and allow for more direct exchange of information between the contributors. In other cases, where the ML/TF risks are diverse and differ between regions, or where the competent authorities have to deal with very specific risks or need to conduct an assessment to justify exemptions on the basis of low ML/TF risks, it may be more appropriate to have targeted, sectoral or thematic risk assessments which the national authorities would then use in developing a national-level understanding of the ML/TF risks.

20. The size and complexity of the country, its ML/TF environment, and the maturity and sophistication of the AML/CFT regime may also influence how a country decides to assess and understand its ML/TF risks. Ideally, a national-level ML/TF assessment should attempt to focus on macro-level risks affecting the AML/CFT regime. For example, it may focus on the potential abuse of sectors rather than of individual institutions, or the adequacy of resources across a linked group of AML/CFT competent authorities rather than individual authorities, and so on. The degree of aggregation or disaggregation of risks to focus on will be country specific.

Comprehensiveness of assessment

21. Regardless of the approach adopted, countries are advised to ensure that their assessment of ML/TF risk is comprehensive enough to provide an overall picture of the national ML/TF risks across the AML/CFT regime. Ideally, this picture should include sufficient breadth and depth about potential threats and vulnerabilities and their consequences to address the purpose and scope of the assessment. The range of threats and vulnerabilities relevant for any particular assessment will thus vary according to the scope of the assessment (national, regional, sectoral, etc.); however, the country will need to ensure that all relevant risks are taken into account when the results from different types of assessments are combined to derive national-level ML/TF risks. Where information gaps exist or difficulties in reaching conclusions arise, it is useful if these can be recognised in the risk assessment and then become areas where more work is required in the future. In addition, the uncertainty caused by the lack of information may itself raise the risk profile of the issue under consideration. In seeking to develop a comprehensive picture, those in charge of the ML/TF risk assessment need to identify and acknowledge these limitations as they make a determination of the risks that can be assessed. Future risk assessments may be able to seek new or alternative sources of information that will permit assessment of areas that could not be adequately or fully assessed in an earlier work.

10 Again, UNODC (2010) mentioned above may be relevant in this regard.

2.3 Need for high-level commitment to the ML/TF risk assessment process

22. Before conducting an ML/TF risk assessment, it is essential that there be the political will to carry out this work and ensure that the objectives of the assessment can be achieved. This political will may be demonstrated in a clear commitment from high-level government officials to the ML/TF risk assessment exercise. These officials will need to recognise, understand and acknowledge any ML/TF risks that exist within their country and how these risks may be distinct from larger criminal or terrorism related threats. Situations where government officials (or competent authorities) purposely fail to identify ML/TF risks in their country (or they deliberately determine certain risks as low level) because they believe that acknowledgement of a higher risk level may damage their reputation or may have a negative effect on investment within the country and its financial sector need to be avoided.[11] Appropriate judgment and balance are therefore important in the conduct of the national ML/TF risk assessment process to prevent the process from becoming unduly influenced by or subordinate to a particular policy approach, legislative reform, agency agenda, resource injection, or lobbying by a specific stakeholder.

[11] Examples of situations where ML/TF risks are often not acknowledged include those where a country itself may have little criminal or terrorist activity but its vulnerabilities attract foreign funds for laundering or financing activity or its residents send funds abroad to support foreign terrorists and terrorist groups.

3. ORGANISATION AND INFORMATION

3.1 Planning and organisation of the ML/TF risk assessment

23. In establishing a ML/TF risk assessment process, some countries may choose to establish a more formal inter-agency working group or the like to oversee their risk assessment process. Round-table discussions, working groups of experts and taskforces of relevant agencies and bodies are other examples of how such a process may be organised. It is useful if the process is as inclusive and co-operative as possible. However, ideally there should be a clear determination and designation of the specific agency, organisation or "task force" in charge of leading and co-ordinating the process. See Annex III which contains examples of national-level assessments for specific ways that countries have organised their assessments.

24. As mentioned in the previous section, the purpose and scope of the particular assessment will likely determine the composition of the risk assessment "team". Meetings, interviews, data gathering, and analysis related to national-level ML/TF risks can be a lengthy process, particularly if there is disagreement among competent authorities on the threats and vulnerabilities. A clear project plan describing the process, roles and responsibilities of various partners for identifying, assessing and understanding the country's ML/TF risks may therefore be useful. In addition, an appraisal of likely resource requirements needed to undertake the ML/TF risk assessment may be beneficial.

25. There are a variety of processes through which a country may reach an informed understanding of the risks it faces – in a particular situation or overall. This includes top-down approaches (resulting from a single, co-ordinated framework or system) and bottom-up (building a national assessment from a patchwork of assessments with a smaller scope). It also includes organic processes which may develop an understanding of risk incrementally, for example by starting with a limited or specific focus assessment and gradually expanding it whilst learning from the experience of the preceding work.

3.2 Sources of information

Contributors to the risk assessments

26. While some aspects of the ML/TF risk assessment may be conducted through a single agency process, in most cases, it is unlikely that one organisation by itself possesses all necessary information and data to adequately perform such a task at the national-level. It is therefore advisable that a national-level ML/TF assessment exercise involve a broad range of relevant departments, agencies and other organisations within the government (federal and other levels as applicable) that have AML/CFT responsibilities, expertise or both. This includes those with knowledge of the types and scope of proceeds-generating offences, those that can identify AML/CFT regime vulnerabilities and those with other critical related information. Contributors that may provide essential input to the national-level ML/TF risk assessment process include the following (see also Figure 1):

- *Policy-making bodies*: Policy making bodies should, where relevant, be included in the conduct of a risk assessment – not necessarily as providers of information, but as the principal users of risk assessments – in order to ensure that risk assessments adequately address high-level questions and that any implications of the risk assessment for the revision of national AML/CFT policies are identified. They have a particular role to play in helping frame the scope of the risk assessment exercise.
- *Law enforcement and prosecutorial authorities* (including police, customs/border control, and criminal intelligence agencies where appropriate): These operational authorities may be able to provide information on specific cases involving the particular area under assessment and may also assist, where possible, in estimating amounts of proceeds of crime based on information on predicate offence. They thus are likely to play a central role as a source of information for the process. They may also have relevant statistics on ML/TF investigations, prosecutions and convictions, assets seized / confiscated / repatriated / shared and other (international) co-operation requests or hold information about criminals' *modus operandi* obtained during the course of an investigation. They may also be able to provide information on new trends and risks detected through their investigations as well as assist in identifying vulnerabilities.[12]
- *Intelligence and/or security services*: These agencies may be particularly relevant to assessments of terrorism and terrorist financing, where much of the available information on threats may come from intelligence sources[13]. Such agencies may also function as centres of expertise on intelligence analysis, and can provide external review or validation of risk or threat assessments using intelligence analysis and assessment methodologies, where these are available. They may also be able to assist in identifying vulnerabilities.
- *Financial intelligence units*: On the basis of the suspicious transaction reports (STRs) and other information it receives and the strategic analysis it conducts, the FIU is ideally placed to identify threats, vulnerabilities, ML/TF techniques, methods and trends, including new patterns[14]. FIUs may be able to extract from their databases information on specific products or transaction types that can be either converted into sanitised cases and/or

12 Some of this information may be available from other authorities such as Justice Ministries and other agencies.

13 However, this may involve information of a sensitive nature which could limit the exchange by intelligence or security services.

14 See INR 29 which describes the role of the FIU in conducting strategic analysis and its role in helping establish policies and goals for other agencies within the AML/CFT regime. At the same time, it may be advisable not to rely too heavily or solely on FIU statistics as these often derive from suspicion about potential ML or TF activity rather than actual cases.

aggregated to reveal a trend. This information can be supplemented by statistics on the reporting of transactions by the reporting entities.

- *Regulatory and supervisory authorities* (including, for example, self-regulatory bodies and any FIUs with such responsibilities) often have the benefit of having a good picture of the institutions regulated for AML/CFT within their countries. Through their AML/CFT inspection and monitoring, either on-site or off-site, they gain a unique knowledge of specific vulnerabilities associated with types of institutions, products, transactions (including those of a cross-border nature) and customers that can be associated with ML/TF and are able to assess a sector's policies, procedures and controls. They are therefore in a position to provide views on whether a particular risk is being adequately identified and managed.
- *Other authorities* such as Foreign Ministries (for example, threats identified by the UN) or statistics agencies may also hold information that can inform the risk assessment exercise and could participate directly or indirectly. Likewise, agencies that may have information about particular criminal activities or predicate crime may also be able to contribute (for example, welfare ministries in relation to welfare fraud, tax authorities in relation to tax crimes, anti-corruption agencies in relation to corruption etc.).
- *International and foreign partners*: FATF-style regional bodies (FSRBs) of which a country is a member may also be a useful source of information on risk, in particular regarding work carried out elsewhere in the region to identify and understand risk. Similarly, foreign partners, such as authorities from other countries, may also be a potential source of information.

Involvement of the private sector and other actors

27. Private sector involvement may also be valuable in building a complete picture of national ML/TF risks and may benefit the assessment process in a number of ways – as either as a source of information or by having representatives participating directly in some aspects of the process if the country considers that appropriate. It is also important to consider that sometimes the private sector may have commercial interests that might preclude a completely impartial view of ML/TF risk. Therefore, while the private sector may not in all countries be an active participant in the national ML/TF assessment, it may be the best source of information in many areas. Contributors from the private sector that may provide essential input to the national-level ML/TF risk assessment process include the following:

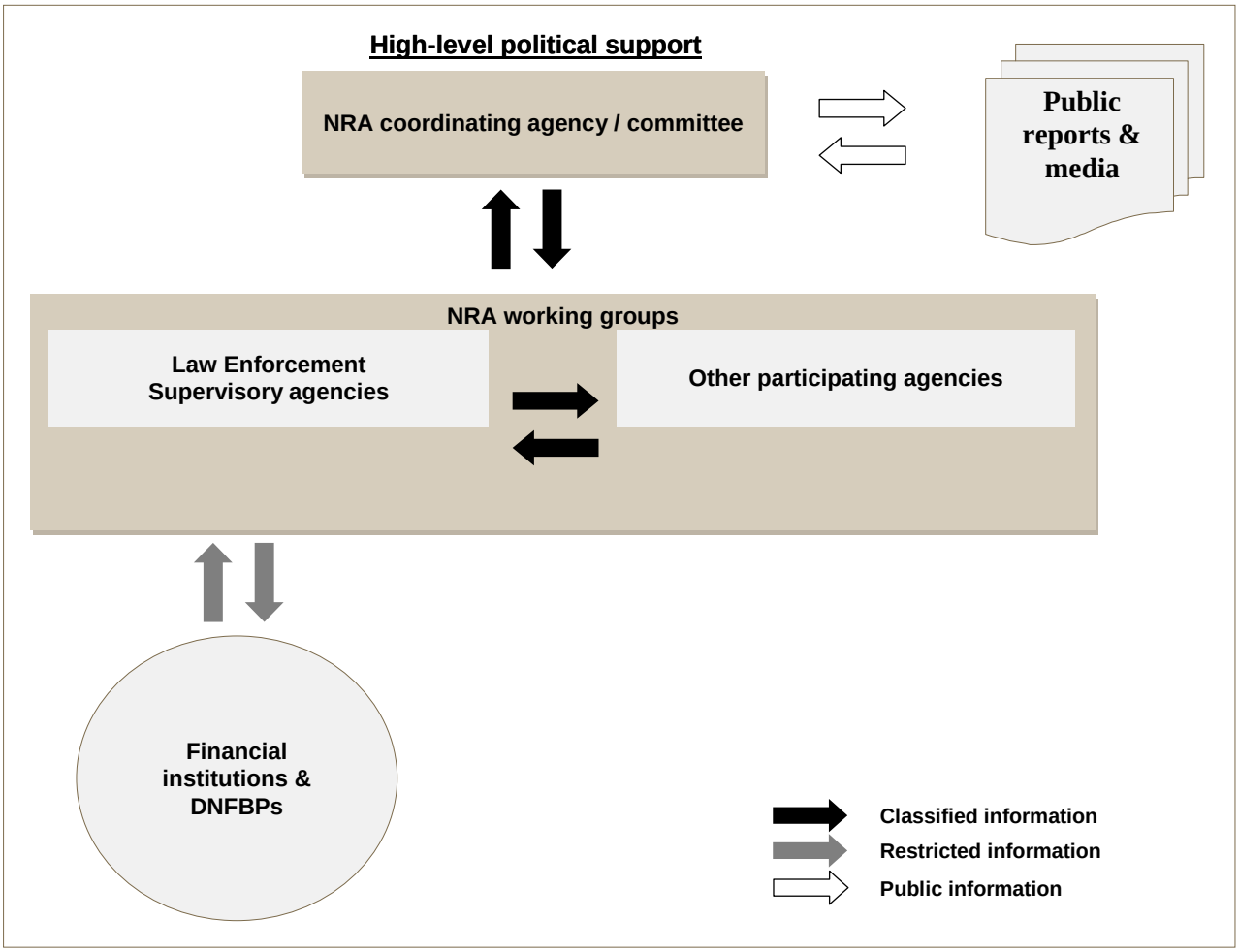
- *Financial institutions and DNFBPs:* When applying the risk based approach to implementing AML/CFT preventive measures, financial institutions and DNFBPs may have already conducted ML/TF risk assessments of their own, and such assessments could also be an important contribution to national-level assessments. More generally, financial institutions and DNFBPs and their staff or representatives may have valuable information on the structure, organisation and size of sectors, their customers as well as the

features and characteristics of particular financial products to help with determining the level of risk presented and to assist in identifying vulnerabilities. As stated in the introduction, the private sector is also a potential key user of any ML/TF risk assessments conducted at national level. It should be noted as well that Recommendation 1 now requires countries to have mechanisms to provide appropriate information on the results of national ML/TF risk assessments to financial institutions and DNFBPs.

- *Industry associations and self-regulatory bodies (SRBs)* with a broad and representative membership in the area of the assessment may provide essential aggregated statistics, such as particular types of transaction volumes and industry-wide information.
- *Other actors*: researchers, criminologists, industry associations, private sector experts (for example, practitioners or others with in-depth knowledge of specialised financial activities), risk management experts, non-government organisations and civil society, academics and other international experts/specialists can provide their perspectives, for example, on what constitutes a "cash intensive" business or economy, produce reports and provide analysis related to ML/TF and predicate crimes. It may be very useful to develop risk assessment methods and the monitoring of the risk assessments by actors with expertise in scientific research.
- *Criminals* could also be a valuable source of information, particularly in jurisdictions where they are given the incentive to "repent" or share information in return for favourable treatment in the criminal justice system. They can explain the reasons why one sector or product or transaction or (more broadly) *modus operandi* was chosen rather than another. While it may be difficult to obtain such information from them directly, there may be indirect methods such as obtaining copies of research into their behaviour or working with prison or custodial authorities to obtain valuable information that they may hold. Court reports, sentencing and transcript records can also be a rich source of information on the motives and methods used by money launderers and terrorist financiers.

28. As a targeted ML/TF risk assessment may focus on a specific sector, only a small number of private sector representatives (for example, from an industry association or SRB) might be involved. A comprehensive national risk assessment on the other hand is of a larger scope and could attract more participation from a wider segment of the private sector. Time and resources to co-ordinate input and obtain agreement among participating bodies need to be considered when planning to undertake large-scale ML/TF assessments that involve extensive consultation.

Figure 1. **Interrelationships between various contributors to the risk assessment process**



Information and tools required for ML/TF risk assessments

29. The quality of the risk assessment exercise depends largely on the types and quality of data and information available. While quantitative assessments (*i.e.*, based mostly on statistics) may seem much more reliable and able to be replicated over time, the lack of available quantitative data in the ML/TF field makes it difficult to rely exclusively on such information. Moreover, information on all relevant factors may not be expressed or explained in numerical or quantitative form, and there is a danger that risk assessments relying heavily on available quantitative information may be biased towards risks that are easier to measure and discount those for which quantitative information is not readily available.

30. For these reasons, it is advisable to complement an ML/TF risk assessment with relevant qualitative information such as, as appropriate, intelligence information, expert judgments, private sector input, case studies, thematic assessments, typologies studies and other (regional or supranational) risk assessments in addition to any available quantitative data. Similarly, objective data can be complemented by surveys or information of subjective nature such as perception indexes. Countries may in the long term wish to consider harmonising and further developing their quantitative data collection mechanisms that are used for ML/TF risk assessment in line with the FATF Standards (for example, Recommendation 33) and international best practices. It is essential

that all participating organisations be authorised to share potentially sensitive information. Such information should be received, exchanged and used in accordance with agreed procedures, policies and applicable laws and regulations.

31. Determining the sources of data, type of information, tools, and which analytical techniques will be used is therefore essential in conducting ML/TF risk assessments. In order for a national ML/TF risk assessment to arrive at the most accurate findings, it is advisable that as much analysis and conclusions within the assessment as possible be based on objective information. The information used in a ML/TF risk assessment may be derived from various sources (both qualitative and quantitative). The availability and quality of information will vary considerably by country. Countries, including low capacity countries, with limited data on criminal investigations or financial transactions will still be able to conduct a risk assessment but may need to rely more on expert judgment and international sources of data after they have obtained all available data from national sources. More generally, some officials may find it beneficial to engage independent experts with substantial experience in risk assessment to carry out some aspects of the risk assessment rather than try to carry out the whole process themselves.

32. A national ML/TF risk assessment may conclude that one of the significant vulnerabilities is the presence of information gaps within the AML/CFT regime that need to be closed. Thus, the risk assessment can also reveal the adequacy of the available data and give directions for potential data and information sources, as well as future data collection requirements. A review of the available data and information within a country's AML/CFT regime as an essential component of the ML/TF risk assessment process also helps identify the extent to which any lack of data and information is a systemic vulnerability in the country.

33. Maintaining a consistent approach to the risk assessment process and using the same quantitative and qualitative indicators where possible is important to enable a comparison of findings over time. However, the desire to compare results between one assessment and the other or after periodic updates should not override the need to improve the methodological process or add new data sources as appropriate. Indeed, the experience obtained from conducting an ML/TF risk assessment – when properly documented – may help a country to refine future assessments or adopt an entirely new and more effective approach in subsequent assessments.

34. When looking at money laundering and terrorism financing trends, a country's international financial transactions may also be a key element. Information on cross-border financial flows is a valuable source of data which needs to be considered. In addition, a number of countries have extensive reporting processes on crimes related to money laundering, such as human trafficking or organised crime and some international organisations collate statistics on these and other relevant crimes. These reports can be an important source of information for assessing national ML/TF risks.

3.3 Other planning considerations

Frequency of the risk assessment

35. Recommendation 1 requires that countries assess risks "on an ongoing basis", and that they keep assessments up-to-date. The authority or mechanism designated to assess ML/TF risks in the

country will likely be responsible for ensuring that this obligation is met. Recommendation 1, however, does not specify a particular period of time. Therefore, the frequency with which a risk assessment is updated is determined by the country, based on a number of factors, including how quickly (and how significantly) the risks may change.

36. Following the initial assessment of a specific area, the entire process does not necessarily need to be repeated at pre-specified points in time. However, it is advisable that the authority or mechanism designated to assess ML/TF risks proposes after the first national-level ML/TF risk assessment when the next risk assessment should be carried out, for example, within the next three to five years. It should also be emphasised that carrying out an ML/TF risk assessment should be considered as an evolutionary process. As indicated above, the lessons learned from an initial risk assessment may help to inform subsequent updates or future risk assessments, and this may also be a factor in determining the frequency.

37. Some factors that could also influence the need for updating or conducting a new ML/TF risk assessment process include: when new ML or TF activity causes substantial harms to occur, or new intelligence or typologies become available or where significant changes are made to products and services (including their operating environment). A number of developments (domestically and internationally) may also prompt the need to review a risk assessment:

- Changes in international standards or guidance (for example, FATF recommendations, IOSCO, IAIS, guidance and sound practice papers issued by the Basel Committee on Banking Supervision, UN Conventions, EU legislation).
- Changes in the political, economic or legal framework of a country.
- Developments in other countries' regimes (in particular the country's important trading partners or countries with similar financial sectors or legal systems).
- Issues raised by the private sector (for example, "level-playing field", "countries of concern" not already identified by FATF, new products, services and technologies).
- Open source material or public reports (for example, FATF typology reports) on new ML or TF trends.
- Domestic typologies studies and intelligence received from law enforcement, the FIU and other stakeholders, which may include updates on the vulnerability of a product or service.
- Information about trends in other countries (by means of international conferences, regular information exchanges, etc.).
- The cycle of mutual or self-evaluation may also be an important consideration for countries in deciding when to conduct or update their risk assessment.

Documentation of methodologies and processes used

38. Regardless of the method or process used to conduct the ML/TF risk assessment exercise, it is advisable that the designated authority or mechanism responsible for assessing a country's ML/TF risks record sufficient information about the methodologies and processes to be used. This is to ensure that all parties involved in the process are aware of their obligations and responsibilities and to assist with demonstrating to other stakeholders, including assessors, how the risk assessment was conducted. Such an approach is also appropriate for the purposes of transparency and accountability.

39. While not all the information and analysis of the risk assessment may be shared broadly, it is essential that the designated authority in charge of co-ordinating the process ensure that adequate records of the data, information, analysis and conclusions are kept securely. Such records allow for the preservation of institutional memory and in explaining the rationale for past risk-related policy decisions, permit future updates, and ensure the consistency in future risk assessments endeavours. Countries can use this body of information to inform AML/CFT assessors about the adequacy of their risk assessment process, subject to restrictions on sharing sensitive information.

Supra-national risk assessments

40. Assessments conducted at a supra-national-level may be of value in country-level or national risk assessments. Such assessments may serve as an additional source of information in conducting risk assessments at the country level and could, for example, help in the identification of threats, vulnerabilities and their consequences. They may also provide a benchmark for certain judgments made in subsequent risk assessments at the country level. It is also worth noting that supranational assessments can themselves be informed by the results of country-level risk assessments.

Links with global ML/TF assessment

41. The FATF Global Money Laundering and Terrorist Financing Assessment was adopted by the FATF in June 2010. The Global ML/TF Assessment provides an overview of the ML/TF threats as identified by the FATF (and therefore on a worldwide or "global" level) along with the ultimate harms that they can cause. The aims of the Global ML/TF assessment are to inform governments, the private sector and international policy-makers about ML/TF threats in order to better manage scarce resources and to take more focused actions against ML/TF. The issues identified in the assessment may be useful to governments when conducting national ML/TF assessments. The Global ML/TF Assessment may therefore provide an important part of the context for any assessments undertaken at national level.

42. Only a few countries have previously carried out national risk assessments, but it is envisaged that the production of national-level risk assessments will become a more important contributor to the Global ML/TF Assessment effort. Therefore there is a two-way relationship between this assessment and national ML/TF risk assessments with each benefiting from information contained in respective assessments.

4. STAGES OF ML/TF RISK ASSESSMENT

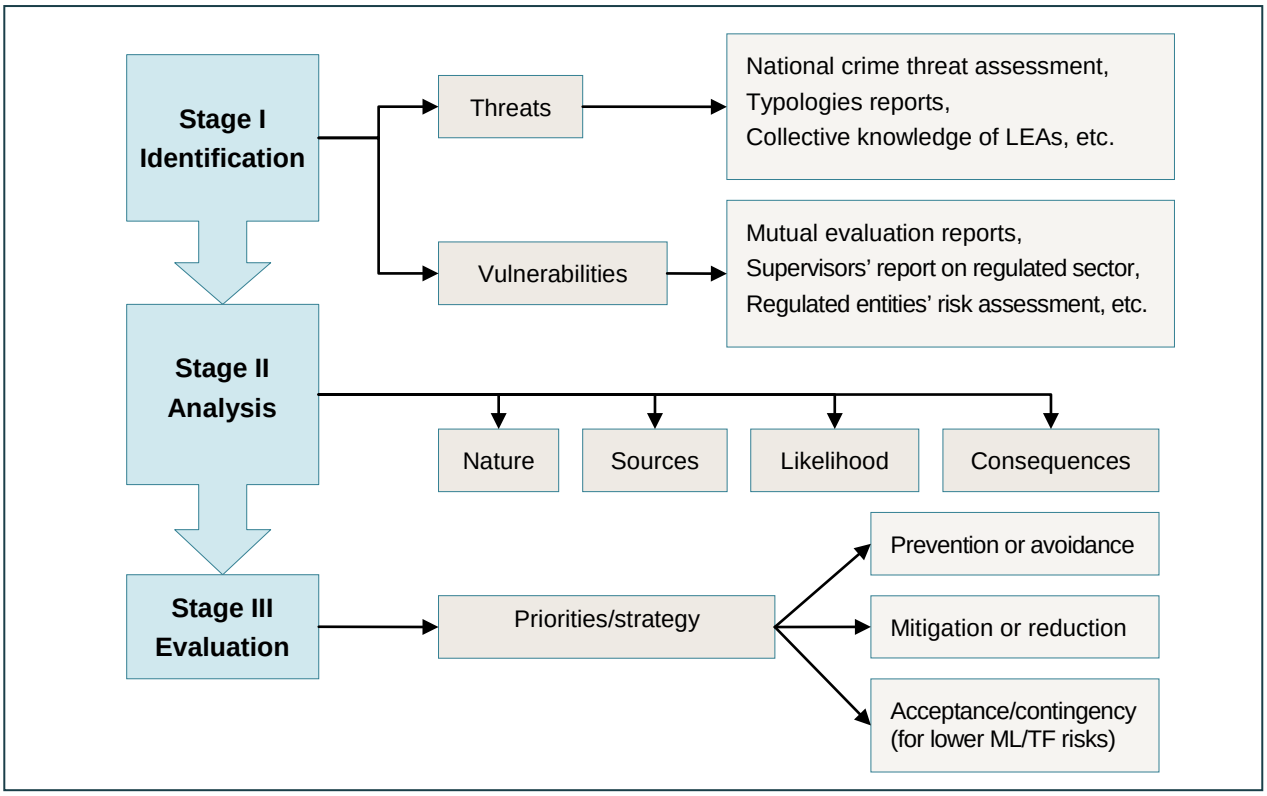
43. The process of risk assessment can be divided into a series of activities or stages: *identification*, *analysis*, and *evaluation*. The three stages are briefly described in this section. For completeness all three stages are described; however, this guidance focuses mainly on the first two. Figure 2 below provides an overview of the ML/TF risk assessment process.

- In general terms, the process of ***identification*** in the context of an ML/TF risk assessment starts by developing an initial list of potential risks or risk factors[15] countries face when combating ML/TF. These will be drawn from known or suspected threats or vulnerabilities. Ideally at this stage, the identification process should attempt to be comprehensive; however, it should also be dynamic in the sense that new or previously undetected risks identified may also be considered at any stage in the process.
- ***Analysis*** lies at the heart of the ML/TF risk assessment process. It involves consideration of the nature, sources, likelihood and consequences of the identified risks or risk factors. Ultimately, the aim of this stage is to gain a holistic understanding of each of the risks – as a combination of threat, vulnerability and consequence in order to work toward assigning some sort of relative value or importance to them[16]. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk and the purpose of the risk assessment, as well as based on the information, data and resources available.
- ***Evaluation*** in the context of the ML/TF risk assessment process involves taking the risks analysed during the previous stage to determine priorities for addressing them, taking into account the purpose established at the beginning of the assessment process. These priorities can contribute to development of a strategy for their mitigation.

15 The term *risk factors* is used to refer to specific threats or vulnerabilities that are the causes, sources or drivers of ML or TF risks.

16 As stated in Section 1 under the descriptions of relevant concepts, a risk assessment at the conceptual level involves gaining a comprehensive understanding of all three components of ML/TF risk (threat, vulnerability *and* consequence). The practical challenges in describing ML/TF consequences in a meaningful way may lead countries to focus first and foremost on identifying ML/TF threats and vulnerabilities. The recognition that there are specific consequences of ML/TF threats and vulnerabilities is nevertheless important, as this component, even if understood at a theoretical level may help in assigning a relative value or importance to various ML/TF risks.

Figure 2. **Overview of the ML/TF Risk Assessment Process**



4.1 First stage: identification

44. After establishing the purpose and scope for the risk assessment exercise, a first step is to identify risks to be analysed. Given that ML/TF risks – as stated earlier in this guidance – are a combination of threats, vulnerabilities and consequences, a good foundation for the identification process is to begin by compiling a list of the major known or suspected threats and vulnerabilities that exist based on primary methods and payment mechanisms used, the key sectors which have been exploited, and the primary reasons why those carrying out the ML/TF are not apprehended and deprived of their assets. The identified ML/TF threats or vulnerabilities should of course relate to the purpose and scope of the assessment and this will also influence whether they are more micro or macro in focus.[17]

45. At this initial stage, the list may be broad or specific, be based on actual or known typologies, or drawn from a more generic list of types of cases or schemes or circumstances involved in the ML or TF processes. For ML/TF threats, the development of a list may be facilitated by having access to, for example, national crime threat assessments[18], typologies reports, as well as the collective

17 Decisions will need to be made about the level of aggregation or detail with which the list of threats and vulnerabilities is expressed (along with the risks derived from them), and this will be influenced by the size and complexity of the country. A more focussed ML/TF assessment will typically involve a narrower range risks but it may provide more opportunity for those to be expressed using a higher level of detail than for a national level assessment.

18 Again, the UNODC (2010) mentioned above may be relevant in this regard.

knowledge of law enforcement. Formulating a list of the country's major ML/TF vulnerabilities will typically be informed by the likes of mutual evaluation reports[19] of compliance with the FATF Recommendations[20], reports by supervisors and about vulnerabilities in the regulated sector, risk assessments prepared by regulated entities, and the collective knowledge of the authorities involved in AML/CFT, particularly regarding the existence and effectiveness of any general mitigants or controls that help combat ML/TF (such as limits on cash use in certain transactions) and any weaknesses in how they carry out their responsibilities, including because of a lack of resources. The exercise of establishing this first list of threats and vulnerabilities should consider the full process of ML or TF, including the international/cross-border context. Thus, discussion of ML or TF threats will probably need involvement of appropriate experts who contribute to compiling this initial list of the main or common ML/TF threats and vulnerabilities.

46. ML/TF risks exist when ML/TF threats exploit ML/TF related vulnerabilities. Thus after compiling a list of ML/TF threats and vulnerabilities, the next focus is for those involved in the process to think about how these interact and articulate a list of risks the country faces when combating ML/TF.[21] It should be stressed that something identified on the list at this stage is not automatically classified as having higher (or lower) risk – it has simply been identified as sufficiently relevant to go into mix of risks to be analysed.

47. There are different approaches that may be used at the identification stage. One is based on identifying risk *events*, which involves starting from specific examples of ML or TF events – which may be macro or micro in nature. Under this approach the participants identify the main risk scenarios to analyse. Some examples of specific ML/TF risk events (derived from the threats, vulnerabilities and consequences) identified at this stage might include the following[22]:

- "Organised crime groups place proceeds of crime into the financial system through co-mingling cash with legitimate business takings."
- "Narcotics trafficking groups use cash smuggling to move illegal proceeds over the border."
- "Terrorist group X is known to raise funds via cash donations obtained within the country."
- "Foreign terrorist groups uses domestic NPOs as fronts for terrorist financing activities."

---

19 And detailed assessment reports.

20 Any of these reports may contain outdated information due to the length of time since the last assessment. This material may therefore be supplemented by other material developed through subsequent follow-up or monitoring processes.

21 Some country ML/TF risk assessment processes may wish to move straight to articulating a list of ML/TF risks without identifying threats and vulnerabilities separately

22 See Annex I for a more lists of examples of predicate offences (threats) for money laundering and see Annex II for a list of vulnerability related factors. These may be of assistance in developing lists of threats, vulnerabilities, and consequences during ML/TF risk assessments. It is important to note however that these lists are not exhaustive.

- "Foreign criminal groups launder foreign proceeds of crime in the country by investing in the domestic real estate sector."
- "Criminals and terrorists exploit the lack of information on beneficial ownership and control of companies to obscure or hide links between them and legal persons controlled or owned by them."
- "Terrorists / criminals move funds out of the country via informal money transfer businesses."
- "Financial institutions fail to identify suspicious transactions because of poor monitoring systems."
- "Law enforcement fails to investigate ML due to their focus on predicate crime only."
- "Launderers avoid conviction due to poorly drafted ML laws."
- "Law enforcement are unable to investigate some ML and TF cases due to poor information about beneficial ownership and control of companies used by launderers and financiers."
- "Confiscation of proceeds of crime fails because law enforcement fail to use provisional measures to freeze or seize assets during investigations."

48. Another approach that may be used starts from a macro-level and tends to focus more on circumstances. Under this approach a list of risk factors (relating to threats and vulnerabilities, see Annexes I and II for some examples of risk factors) is identified for analysis. The list can be expanded or narrowed down depending on the scope of the ML/TF assessment.

49. Irrespective of which approach is used for identification, those involved in the process must keep an open mind to ensure that all relevant risks or risk factors are identified so as to avoid inadvertently overlooking key issues that contribute to the country's ML/TF risk. The actual processes used to identify the initial list of risks will vary. Some countries may utilise more formal techniques such as surveys and quasi-statistical analysis of past events or circumstances while others may carry out a brainstorming exercise among appropriate experts to produce a list or perhaps a tree diagram of related events or circumstances. Once an initial list of risks is identified, the assessment process can proceed to the next stage.

4.2 Second stage: analysis

50. *Analysis* lies at the heart of the ML/TF risk assessment process. It is through analysis that the process moves from a mere description of the ML/TF risks facing a country – akin to a situation report – to fuller understanding of the nature, extent and possible impact of those ML/TF risks. As indicated in the introduction, risk can be thought of as a function of *threat*, *vulnerability* and *consequence*. The goal of this step is therefore to analyse the identified risks in order to understand their nature, sources, likelihood and consequences in order to assign some sort of relative value or importance to each of the risks.

51. Ideally, such analysis takes into account the relevant "environmental" factors -- in the broadest sense -- which influence how the risks evolve. These broad "environmental" factors include the general circumstances of the country (for example, relevant political, economic, geographical and social aspects), as well as other structural of specific contextual factors which could influence the way AML/CFT measures are implemented. Determining which environmental factors are relevant to ML and TF (and thus influence the nature, sources, likelihood and consequences of the identified risks) can be assisted by thinking of them in terms of the political, economic, social, technological, environmental and legislative factors that may enable or facilitate the particular risk. In practical terms, many of these factors will have already been identified as among some of the vulnerabilities facing the country (See Annex II).

52. In practice, not all broad environmental factors will be applicable to every ML/TF risk assessment. Indeed, the individual factors will vary from country to country and may evolve over time. It is important to ensure that factors looked at are indeed relevant, and it may therefore be necessary to use some of the methods (surveys, brainstorming) mentioned above to agree on which factors to consider in a particular ML/TF assessment process. In addition, it may become apparent in thinking about some of these factors that certain ML/TF risks might not have been identified at the first stage. As stated previously, the process – even at the analysis stage – should be flexible enough to make adjustments to modify (add to, delete or combine) the risks identified in stage one of the process.

53. Having considered the influence of the broad environmental factors on each identified risk the analysis stage can move on to attempting to determine the size or seriousness of each risk. Often this may mean determining the size or seriousness of the risk in relative terms to other risks. This can be done by using different techniques, for example:

- If doing this holistically, those involved in the risk analysis might collectively rank or categorise each of the identified risks in terms of their degree and relative importance.
- More formal analytical techniques can involve identifying the nature and extent of the consequences of each risk along with the likelihood that the risk may materialise and combining those results to determine a level of risk, which is often presented through the use of a matrix. The actual processes used to identify consequences and determine likelihood can also vary: Some countries may choose to employ more formal techniques such as surveys of experts or statistical analysis of the frequency of past ML or TF risk related activity. Others may choose to rely on the conclusions of a group discussion or workshop to help develop this information.

Understanding the consequences associated with ML and TF

54. In the process of analysing ML and TF risks, it is crucial to have a general understanding of why ML and TF occur. The acts of laundering money and financing terrorism are done to facilitate crime and terrorism more broadly. Profit is fundamental to the goals of most crime and therefore criminals make great efforts to move illegally obtained money and other assets in order to convert, conceal or disguise the true nature and source of these funds. In order for terrorists to carry out

their operations, attacks or maintain an infrastructure of organisation support, the need to have the ability to collect, receive and move funds. The availability of working capital is also fundamental for both criminals and terrorists to sustain their networks.

55. It is equally important to understand the consequences associated with the activity described above. This will assist in reaching conclusions about the relative importance of each identified risk. The consequences of this illicit financial activity are often viewed at the national or international level but also affect the regional, local and individual levels. Both *impacts* and *harms* (which make up consequences) can be further categorised into types, such as physical, social, environmental, economic and structural[23]. From a national perspective, one of the main consequences of ML and TF is that it has a negative effect on the transparency, good governance and the accountability of public and private institutions. ML and TF activity also causes damage to a country's national security and reputation and has both direct and indirect impact on a nation's economy. Box 1 sets out examples of consequences of money laundering, to assist those carrying out ML/TF risk assessments to reach conclusions about the relative importance of each identified risk.

Box 1. **Examples of Consequences of Money Laundering**

- Losses to the victims and gains to the perpetrator
- Distortion of consumption
- Distortion of investment and savings
- Artificial increase in prices
- Unfair competition
- Changes in imports and exports
- Effects growth rates
- Effects on output, income and employment
- Lower public sector revenues
- Threatens privatisation
- Changes demand for money, FX-rates and interest rates
- Increases in FX-rate and Interest rate volatility
- Greater availability of credit
- Higher capital in-flows
- Changes in foreign direct investment
- Risks for financial sector solvency and liquidity
- Profits for the financial sector
- Financial sector reputation
- Illegal business contaminates legal
- Distorts economic statistics
- Corruption and bribery
- Increases crime
- Undermines political institutions
- Undermines foreign policy goals
- Increases terrorism

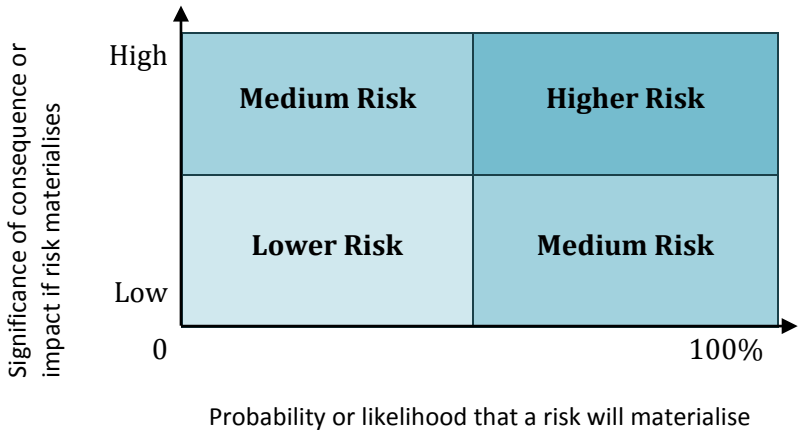
Source: Unger *et al*. (2006). The original source refers to *effects* – however, the term *consequences* as used in this table is consistent with the approach taken in this guidance.

56. A particular challenge especially when using more formal techniques is that ML/TF risks are inherently difficult to describe or measure in quantifiable or numerical terms. It is therefore important to remember that *risk* as we have discussed it in this guidance is a combination of threats, vulnerabilities along with consequences. If the level of risk of the individual risks can be examined according to their consequences or impact and the likelihood of their materialising, then a rough

[23] See FATF (2010), Annex C on "Crime and Terrorism Harm Framework".

estimate of risk level may be obtained. A very simple matrix as applied to a specific risk might be as shown in Figure 3.[24]

Figure 3. **Examples of a Risk Analysis Matrix**



4.3 Third stage: evaluation

57. The last stage of risk assessment is evaluation. It involves taking the results found during the analysis process to determine priorities for addressing the risks, taking into account the purpose established at the beginning of the assessment process. These priorities can contribute to development of a strategy for their mitigation. As indicated in the introduction, this guidance does not attempt to provide a full explanation of this step of the process. For the sake of completeness however, some general details are set out here.

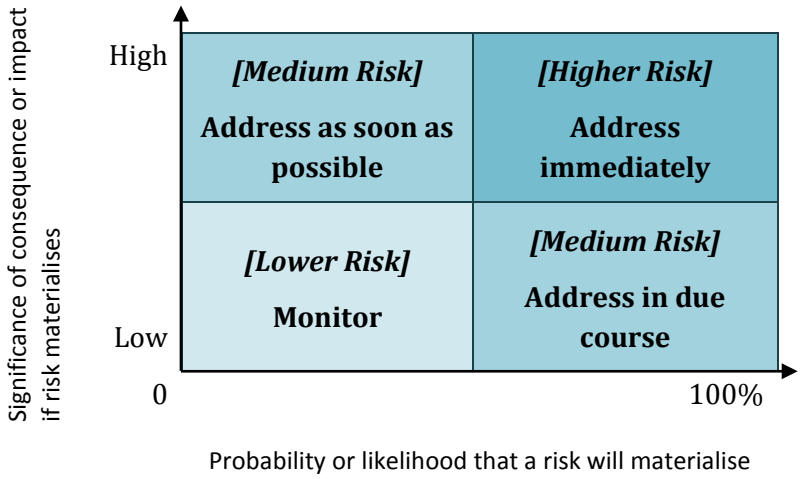
58. Depending on the source, there are a number of methods for addressing (or "controlling") risk, including prevention (or avoidance), mitigation (or reduction), acceptance or contingency planning. In the context of ML/TF risk and the risk-based approach, the most relevant of these methods are prevention (*e.g.*, prohibiting certain products, services, or activities) and risk mitigation (or reduction). The role of evaluating levels of ML/TF risk therefore normally leads to the development of a strategy for addressing the risks. Working from the example in the last section, the evaluation of risk levels for each of the analysed risks could result in courses of action as illustrated in Figure 4 [25], which is provided as a simple example of how the evaluation process might proceed at this stage:

---

24 This example is adapted from UNODC (2010). Note: This example is intended to give a general idea of the thought process at this stage and is not meant to prescribe a particular approach. In some cases, a more detailed matrix might be used in order to indicate a broader range of levels of risk. For example, probability of likelihood could use a 5-step descriptive scale such as *Very likely / Likely / Possible / Unlikely / Very unlikely, and impact or consequence might be described using a 3 point scale such as Major / Moderate / Minor.*

25 This example is adapted from UNODC (2010). See previous footnote.

Figure 4. **Examples of a Risk Evaluation Matrix**



59. According to this example, higher levels of risk might require more immediate action to mitigate it; lower levels of risk might require lesser action or some other response (the example here indicates monitoring). Alternatively, higher levels of risk may indicate systemic or deeply entrenched risks which require a broader response over time. By their nature, such responses generally require consultation (within government and between government and industry, among others), policy development and the implementation of measures, all of which can take time. The example shown here has been kept deliberately simple in order to clearly show the range of decisions that might be appropriate in addressing different levels of risk. A comprehensive ML/TF risk assessment process carried out at the national level might use a more detailed matrix in order to encompass a wider range of potential actions. Also note that, other types of risk matrices than the examples given above or a list ranking of the risks may also work, but the basic principles of the concept of risk as discussed in this paper should be applied.

60. The prioritisation of ML and TF risks at the evaluation stage will assist in the challenge of allocating scarce resources to fund AML/CFT programmes and other public policy and safety efforts. In the budgeting process, it is important to identify and prioritise issues that require attention. The evaluation process helps the authorities make decisions about how best to utilise resources and set priorities for regulatory agencies and the criminal justice system.

61. From an AML/CFT context, countries should implement necessary measures (for example, the FATF standards) and allocate appropriate resources to mitigate the risks which they have identified. In fact, the risk-based approach allows countries to develop a more flexible set of measures in order to target their resources more effectively, including by applying preventive measures flexibly to the financial and other sectors. Based on the risks identified, measures should address how best to prevent the proceeds of crime and funds in support of terrorism from entering into these sectors. Measures to mitigate risk should also address the ways in which these actors can better detect and report this activity. From an operational and criminal justice perspective, measures should be in place to better detect, disrupt and punish those who are involved in this activity.

5. OUTCOME OF RISK ASSESSMENTS

62. The actual results of a risk assessment can take different forms. For the public authorities that are ultimately the main users of the assessment, there is often an expectation that some form of a written report will be produced, although this is not strictly speaking a requirement of Recommendation 1[26]. If the assessment will be presented in report form, decisions on how it will be organised – along with the level of detail – are most usefully made early on the risk assessment process and normally relate directly to the purpose and scope of the assessment. For example, a ML/TF risk assessment with law enforcement or other operational services as the primary users might discuss risks according to the threats (actors and activities) that were the starting point of the assessment. For a report whose primary audience consists of regulators or the private sector, a discussion of the risks grouped according to vulnerability (sector, product, etc.) might be most useful.

63. Regardless of the form and presentation of the ML/TF risk assessment, it should ultimately allow public authorities to make a judgment on the levels of the risks and priorities for mitigating those risks. The policy response can then be made commensurate to the nature and level of the risks identified. It is therefore advisable that the risk assessment contain sufficient information about the source, nature, and extent of each risk to help indicate appropriate measures to mitigate the risk. Thus, the results of national ML/TF risk assessments can provide valuable input in the formulation or calibration of national AML/CFT policies and action plans. This policy decisions may ultimately affect a number of competent authorities and how they carry out their responsibilities (*e.g.*, how financial investigations are conducted). The results of ML/TF risk assessments may also help inform planning for technical assistance on AML/CFT matters by a broad range of donors and technical assistance providers.

Dissemination of assessments outcome

64. Once completed, authorities will have to consider how broadly the results of the risk assessment are to be disseminated amongst the various stakeholders. More specifically, Recommendation 1 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

65. Some ML/TF risk assessments may be considered to contain too much sensitive information to disclose publicly or that they may draw too much attention to the shortcomings in the AML/CFT system of a country. Furthermore, some of the information shared during the course of the assessment could be subject to confidentiality requirements. Nonetheless, appropriate information from assessments should be made available to the private sector to assist it in addressing the current ML/TF risks and new and emerging threats. In certain countries, committees or working groups with vetted private sector representatives have been created to share and discuss risk

[26] Countries will, however, be expected to demonstrate the process, mechanism and information sources used, as well as their understanding of and how they are addressing the identified risks.

assessment information. More generally, it may be helpful to share information – at a minimum – on the main factors considered and the conclusions of the risk assessment process with the private sector. Where the sensitive nature of the information prevents the broad distribution of the full results from the risk assessment report, consideration can be given to circulating sanitised information or summaries, or at least providing information on the methodology used, the findings and the conclusions. This approach could, for example, apply to information provided to assessors in the context of an AML/CFT assessment.

66. A particular objective of a ML/TF risk assessment could be to provide information to the public in order to enhance the general understanding of government AML/CFT initiatives. A typical output of a national ML/TF risk assessment is generally a public document. One challenge to overcome is that some information within the national assessment may be derived from classified or law enforcement sensitive sources. As such, some countries produce a non-classified version for the public.

ANNEX I. ML/TF RISK FACTORS RELATING TO THREAT

As mentioned in the Guidance, having an understanding of the environment in which predicate offences are committed and the proceeds of crime are generated to identify their nature (and if possible the size or volume) is important in order to carry out an ML/TF risk assessment.

The following is a list of crime categories that may be useful in building a picture or estimate of ML/TF threats. This list is not exhaustive, and the individual categories should be viewed as examples and may be complemented in accordance with the purpose and scope of the assessment.

Consideration of all stages of ML

- Placement
- Layering
- Integration

Consideration of all stages of TF

- Raising / collecting funds
- Moving funds
- Using funds

Threat Factors[27]

- Nature and extent of relevant domestic criminal activity (*i.e.*, predicate offences).
- Types of predicate offences.
- Amounts of proceeds of crime generated domestically.
- Physical cross-border in and outflows of proceeds of crime.
- Amounts of proceeds of crime generated abroad and laundered domestically.
- Sources, location, and concentration of criminal activity, including within illegal underground areas in the economy.
- Nature and extent of relevant domestic terrorist activity and terrorist groups.

27 See section on the following page for a list of categories of proceeds of crime / criminal offences that may be useful in looking at threat factors.

- Nature and extent of terrorist activities and groups in neighbouring countries, regions, or sub-regions.

The following is a list of criminal activities organised into categories and sub-categories that may also be useful in building a picture or estimate of threat (in the proceeds of crime environment). This list is not exhaustive, and the individual categories and subcategories should be viewed as examples.

Predicate Crime Categories for ML Crime Categories and Sub-Categories [Source: IMF]

Participation in an organised criminal group & racketeering

- Sophisticated organisations (*e.g.*, mafia, yakuza)
- Drug organisations
- Motorcycle gangs
- Street gangs
- Other

Terrorism and terrorist financing

- Raising funds from criminal activities
- Raising funds from "legal" or apparently lawful activities
    - Willing Donors using "Legal" Fundraising (*e.g.*, NPOs)
    - Deceptive Use of "Legal" Fundraising (*e.g.*, NPOs, donors unaware of TF use)
    - Donated from legal income (*e.g.*, salaries & profits)
- Other

Trafficking in human beings and migrant smuggling

- Trafficking (involuntary)
    - Inwards
    - Outwards
- Migrant smuggling (voluntary)
    - Inwards
    - Outwards
- Other

Sexual exploitation, including sexual exploitation of children

- General - unclassified
- Illegal prostitution
- Sexual slavery
- Procuring sexual activity with minors

- Selling/distributing illegal pornographic material
- Selling/distributing illegal pornographic material involving minors
- Other

Illicit trafficking in narcotic drugs and psychotropic substances

- Cocaine
- Marijuana/Cannabis
- LSD
- Ecstasy
- Meth/Amphetamines
- Heroin/Morphine/Opium
- "Magic" mushrooms
- Other

Illicit arms trafficking

- Small arms/guns
- Light weapons
- Larger Military hardware
- Ammunition
- Weapons of mass destruction
- Other

Illicit trafficking in stolen and other goods

- Stolen goods (NB: only to extent not captured under *e.g.,* theft)
- Gems
- Precious metals
- Radioactive materials
- Cultural goods
- Other

Corruption and bribery

- Bribery - major
    - Friendly GST/tax assessments
    - Avoiding investigation/prosecution
    - Procurement contracts
    - Permits/permissions/licenses
    - Other
- Graft - minor
    - Police
    - Traffic Police

    - Customs Officers
    - Licensing/Permit officials
    - Other
- Embezzlement/misappropriation (theft)
    - Central/federal government
    - Local/state/county etc. government
- Bribery of private sector
- Bribery of foreign officials
- Bribery or embezzlement - international organisations
- Illegal lobbying and political campaign financing
- Other

Fraud

- Against government - General
- Against government - VAT/GST fraud
- Embezzlement/misappropriation (excluding from government by officials)
- Lending fraud (*e.g.*, mortgage fraud)
- Payment instrument fraud (*e.g.*, credit card, check fraud)
- Insurance fraud
- Healthcare fraud
- Benefit fraud
- Vendor, supplier & procurement fraud
- Confidence tricks/scams
- False billing/invoicing
- Cyber & Internet selling frauds (*e.g.*, "phishing")
- Investment frauds (*e.g.*, Ponzi & pyramid schemes)
- Other fraud

Counterfeiting currency

- Local currency
- Foreign currency
- Other

Counterfeiting and piracy of products

- Illegal parallel imported products
- Patents/copyright/trademark infringement
- Clothing and shoes
- Accessories: bags/sunglasses/watches etc.
- Books

- Information technology
- CDs/DVDs, etc.
- Cigarettes
- Foodstuffs
- White ware & other electricals
- Pharmaceuticals
- Of collectibles (*e.g.,* wine, antiquities)
- Software
- Other

Environmental crime

- Illegal fishing
- Illegal logging
- Illegal dumping/polluting
- Illegal mining
- Other illegal extraction
- Illegal trading in endangered species (CITES)
- Illegal construction
- Other

Murder, grievous bodily injury

- Murder - for hire/contract killing
- Murder - motive is profit (*e.g.,* insurance claim)
- Grievous bodily injury- for hire or to derive funds or assets
- Other

Kidnapping, illegal restraint, and hostage taking

- Kidnapping/abduction for profit
- Hostage taking for ransoms
- Other

Robbery or theft

- Burglary - commercial
- Burglary - domestic/residential
- Theft/stealing/larceny
- Theft of motor vehicles (including car-jacking)
- Theft from motor vehicles
- Shoplifting
- Pick pocketing
- Bank robbery

- Pilfering/embezzlement (theft by employee)
- Robbery/mugging (including armed robbery)
- Cyber theft (*e.g.*, transferring bank balances through illegal account access)
- Other

Smuggling

- Prohibited imports
- Cigarettes
- Alcohol
- Cash smuggling of "clean" money (including dirty money would be double counting)
- Foodstuffs
- Prohibited exports
- Fuel
- Other

Extortion

- Blackmail
- Protection money/rackets
- Other

Forgery

- Of financial assets
- Philatelic forgery
- Of other documents
- Fake passports
- Fake ID/driver licenses
- Of art
- Other

Piracy (i.e., maritime)

- Theft from piracy
- Extortion or ransoms from piracy
- Other

Insider trading and market manipulation

- Insider trading
- Traded markets - market manipulation
- Anti-trust/cartel or anti-competition violations
- Boiler room scams
- Other

Tax & excise evasion

- Personal income tax
- Withholding tax
- Corporate income tax
- On illegal income sources
- Sales/turnover tax, VAT
- Customs/excise under invoicing - exports
- Customs/excise under invoicing - imports
- Customs/excise false declaration of quantity & product
- Sprits, tobacco, fuel excise evasions
- Gaming machine taxes and excise evasions
- Excise evasions related to counterfeit and piracy of products
- Other excise evasions
- Departure taxes & fees
- Death & estate duties
- Stamp Duty
- Capital gains taxes
- Real estate rental etc. taxes
- Informal sector
- Illegal transfer pricing
- Other

Illegal gambling

- Illegal lottery
- Illegal betting/bookmaking
- Illegal gambling houses/casinos
- Illegal online gambling
- Other

Money laundering

- Of foreign proceeds of crime

Other Proceeds Generating Crimes

- Computer crime
- Illegal trading of goods and services
    - Alcohol and tobacco
    - Pharmaceuticals, including internet pharmacy
    - Anabolic steroids
    - Party and other "non-narcotic" drugs

- Antiquities

- Illegal carrying out of a regulated/licensed business
  - Loan sharking/illegal lending
  - Illegal remittance activity
  - Illegal/prohibited FX dealing or money changing
  - Other illegal/prohibited financial services
  - Illegal professional services (*e.g.*, accounting, legal etc.)
  - Illegal health related services (*e.g.*, abortions, dentistry, donor tissue operations and trading etc.)

ANNEX II. ML/TFRISK FACTORS RELATED TO VULNERABILITIES

In order to understand the ML/TF risks facing a country, the relevant vulnerabilities need to be identified. This annex contains a longer list of examples of factors that may be considered at this stage of the ML/TF risk assessment to help identify relevant vulnerabilities. They have been generally arranged according to the analytical framework known as "PESTEL" (an acronym based on the first letters of the major categories: political, economic, social technological, environmental and legislative). This list is neither exhaustive nor binding, nor would these factors apply in every country's ML/TF risk assessment and they should be applied in the context of each country[28].

Political factors

- Structure of the political system
- Stability of the present government
- Level of political commitment for AML/CFT programmes
- Level of political commitment to fighting crime
- Unaddressed history of terrorism financing activity
- Prevalence of organised crime, especially if involved in illicit drug production, illicit drug trafficking, kidnapping for ransom, extortion, intellectual property crime
- Presence of illicit small arms trade
- Prevalence of smuggling networks
- Presence of individuals, groups or organisations that support or promote violent extremism
- Weak government reach in some areas of the country, particularly border areas; porous borders
- High levels of corruption
- Adequacy of human, financial, and other resources of competent authorities
    - Inadequate resources
    - ML/TF not a national priority
    - No ML/TF risk assessment conducted by the authorities
    - Reluctance to acknowledge ML/TF risk
    - Lack of specialised training
    - Lack of commitment of financial sector, including low levels of reporting and/or lack of quality of STRs

28 Some of the examples are taken from UNODC (2010).

- Financial sector not sufficiently concerned or incentivised regarding vulnerability to ML-related reputational risk
- Requirements of AML/CFT regime not well understood or implemented by financial institutions and DNFBPs
- Inadequate resources allocated to regulation of NPOs, given the risk level identified
- Inadequate resources allocated to address the issues on identify beneficial owners of foundations, associations and other similar entities, such as trusts

- Effectiveness of operations of competent authorities
  - Authorities' capabilities to suppress crime generally, and predicate offences to ML/TF specifically
  - Systemic weaknesses in law enforcement, and in authorities' efforts to counter crime generally, in particular ML/TF
  - Limited or non-existent ability of intelligence and law enforcement engaged in combating ML or TF to use financial information in their investigations
  - Inadequate co-ordination and information-sharing among law enforcement and intelligence agencies involved in combating ML/TF
  - Inadequate co-ordination among national authorities involved in combating ML/TF
  - Significant differences in procedure among competent authorities responsible for combating ML/TF
  - Lack of capabilities of financial intelligence unit (FIU) to process the reports that it receives
  - Lack of capabilities of law enforcement authorities (LEAs) to suppress ML or TF, which might result in ML or TF not being detected or investigated adequately
  - Lack of inter-agency cooperation that impedes AML/CFT processes and operations
  - Lack of capabilities of the prosecutors, the judiciary, and the prison system to deal with ML or TF related crimes, including weaknesses in the law, and other weaknesses that mean that offenders are not prosecuted, convicted, or sanctioned adequately or deprived of their assets or funds
  - Weaknesses in the authorities' ability to gather and share information due to a lack of capacity or legal privilege

- Inability to obtain convictions for ML/TF and related offences
- Lack of an operational FIU or FIU ineffective; inability or lack of capacity to examine STRs
- Lack of engagement or reluctance to engage regionally or internationally on AML/CFT issues, including on requests for assistance
- Ineffective border controls
- Border and immigration officials lack access to INTERPOL I-24/7 global police communication system
- Weak cash courier control at border points
- Weak AML/CFT oversight
- Government does not conduct regular reviews of terrorism financing risk in its NPO sector

Economic factors

- The type of economic system
- The amount of regulation within the economy
- Average earnings of the population
- Currency exchange rates
- Cost of services
- Size of the financial services industry
- Large, complex economy, or both (perhaps making it easier for ML/TF operations to go unnoticed)
- General opacity of the financial system
- Composition of the financial services industry[29]
    - Products, services, and transactions
        - basic information on sectors or products
        - existence of those that facilitate speedy or anonymous transactions
        - cash transactions and cross-border funds transfers
        - delivery channels
        - existence of high-risk correspondent relationships between banks

[29] See also the list of financial institutions and services in later in this Annex.

        - existence of measures to facilitate fiscal optimisation by non-residents (tax haven)
    - Customer
        - types and ranges of customers (*i.e.,* entities, persons, etc.)
        - nature of business relationships
        - existence of higher risk customers
        - adherence to regulatory provisions applicable to customers
        - adherence to any restrictions on customer transactions
    - Geographic
        - business and customer base in specific geographic areas
        - non-residents
        - customers from geographic area of concerns
        - adherence to any requirements in other countries
        - trans-national or cross-border movements of funds
- Ownership/ control of financial institutions and requirements concerning the identification of beneficial owners that are non-residents
- Corporate governance arrangements in financial institutions and the wider economy
- Nature and role of legal persons and legal arrangements in the economy
- Nature, existence, and size of sectors for legal persons and legal arrangements
- Nature of payment systems and the prevalence of cash-based transactions
- Cash-based economy with large informal sector; high percentage of cash outside legitimate banking system, especially relative to comparable countries
- Strict application of financial institution secrecy and other secrecy – including professional secrecy
- Geographical spread of financial industry's operations and customers
- Economic ties with jurisdictions at high risk of experiencing terrorism, political instability, or both
- Presence of NPOs active in overseas conflict zones or in countries or regions known to have a concentration of terrorist activity

- Presence of NPOs raising funds for recipients in a third country which are part of an organisational structure that engages in violent or paramilitary activities
- Opaque relations between grantees and NPOs disbursing funds or resources to grantees, *e.g.,* grantees are not required to disclose to the NPO how funds are used; no written grant agreement; NPO does not perform grantee due diligence, or due diligence is random and inconsistent; NPOs may disburse large sums for unspecified projects selected by the grantee.
- Effectiveness of financial institutions and DNFBPs in implementing the AML/CFT obligations or control measures
    - Customer due diligence
    - Ongoing due diligence, including transaction monitoring
    - Reporting measures currently performed
    - Internal controls
    - Record-keeping

Social factors

- The demographics of the society
- Extent of social inclusiveness
- Significant population shifts
- The ethnic diversity of the population
- Cultural factors, and the nature of civil society
- Areas of social, ethnic or political conflict
- Cultural immigrant, emigrant or religious ties with jurisdictions at high risk of experiencing terrorism, political instability, or both
- Low level of consultation / co-operation between government and financial sector
- Affiliates of banks circumvent international prohibitions that screen transactions for terrorists, drug traffickers, rogue jurisdictions and other wrongdoers
- Bank personnel not required to routinely share information among affiliates to strengthen coordination
- Requirements of AML/CFT regime not well understood or implemented by financial institutions and DNFBPs

Technological factors

- Use of transportation
- New communication methods

- The use of technology in money transfer
- Introduction and use of new payment methods

Environmental and geographical factors[30]

- Global environmental factors such as availability of water, global warming, etc.
- The use and re-use of resources
- Impact of the local environment on crime such as housing, security etc.
- Impact of environmental legislation

Legislative factors

- Criminal justice system and legal environment
- Ease with which new legislation can be passed
- Review process for current legislation
- Impact of international standards on national legislation
- Strengths and weaknesses in legislation combating serious and organised crime
- Strengths and weaknesses in current AML/CFT legislation
    - AML/CFT preventive controls, including AML/CFT specific supervision and monitoring, that collectively do not deter ML or TF nor result in it being detected if it does occur
    - AML/CFT cross-border controls and international cooperation
    - Jurisdiction not a party to the International Convention for the Suppression of the Financing of Terrorism, the United Nations Convention against Transnational Organised Crime and its Protocols, and/or the United Nations Convention against Corruption
    - Adherence to international standards or conventions applicable to the specific sector or product
    - ML/TF not criminalised or inadequately criminalised
    - Incomplete coverage of predicate offences to ML
    - ML/TF not criminalised as a standalone offence
    - TF not a predicate offence to ML offence
    - TF not criminalised unless linked to a specific terrorist act
    - TF only criminalised in relation to the treaty-based offences

30 Certain major categories provided in this example may not be relevant in all ML/TF assessments.

- No measures or inadequate measures to freeze without delay terrorist funds and assets
- Freezing of terrorist funds does not extend to other terrorist assets
- No legislation denying safe haven to those who assist or commit terrorist acts (laws on modalities of inter-State cooperation, extradition, mutual legal assistance, transfer of criminal proceedings, etc.)
- Government has not reviewed its own policies, legislation and other tools in respect of terrorism financing risk in the NPO sector and taken steps to address shortfalls
- Regulation of charitable donations does not cover overseas donations
- Lack of early warning arrangements with other jurisdictions on CFT
- Financial sector not prohibited from conducting relationships with shell banks or shell companies
- Adequacy of AML controls
    - Customer due diligence
    - Ongoing due diligence including transaction monitoring
    - Reporting measures currently performed
    - Internal controls
    - Record keeping
    - Lack of regulation on beneficial ownership
- Lack of guidance to relevant authorities on beneficial ownership
- Limited or absence of risk-based approach guidance on AML/CFT provided by regulatory, oversight and supervisory authorities
- Limited regulation of money or value transfer systems
- Entities not registered and size of sector unknown
- No system of registering or licensing service providers; difficult to take enforcement action and thereby to formalise flows of funds

- Any non AML/CFT controls that apply to entities that can be abused for ML or TF, including general supervision or monitoring
- Any non-AML/CFT related cross-border controls, including general border security
- Extent and efficacy of compliance audits
- Enforceability of rules or guidance
- Existence of a regulator or supervisor
- Links with other financial intermediaries
- Legal or other constraints on products, services, transactions
- Coverage or requirements in other countries

The following table provides a generic list of entities /sectors that may be useful in building a list of the ML/TF vulnerabilities that can be exploited in regulated entities. In particular, it may be worth using such a list to think about vulnerabilities in the context of types of products and services offered by each type of institution or firm and the adequacy of their AML/CFT controls. This list is not exhaustive, and the individual sectors / entities included here should be viewed as examples.

Table 1. **Institution and firm categories by sectors**

Sector	Categories of institutions and firms
Banks and credit institutions	*All banks or commercial banks (including: foreign banks, government-owned banks, merchant banks, special purpose banks)*
	All offshore banks (offering services exclusively to non-residents)
	Building societies, cooperatives and credit unions
	Central bank WITHOUT retail base
	Central bank WITH retail base
	Finance companies
	Savings institutions (including postal savings service)
	Microfinance deposit takers
	Merchant banks
	Shell banks
Securities industry	*Advisers*
	Fund and asset managers (including mutual funds)
	Futures (including commodities) & derivatives brokers and dealers
	Markets, registries & exchanges
	Securities firms (brokers, dealers and other companies)
	Superannuation and pension companies

Sector	Categories of institutions and firms
	Other
Insurance industry	*Life insurance agents and brokers*
	Non-life insurance agents and brokers
	Non-life insurance companies
	Offshore insurers
	Superannuation and pension companies
	Other Insurance
Money services businesses (MSBs)	*Card issuers/E-payment (credit, debit, E-cash/money etc.)*
	Check issuers and cashers
	Foreign exchange dealers (including bureaux de change and money changers)
	Money remitters and transfer agents (including any postal service that offers this service)
	Undertaking of bill payment business
	All (Other) MSBs
Other financial institutions	*Hire purchase companies*
	Mortgage providers
	Other lenders
	Other specialist financial institutions (such as development FIs)
	Pawnshops (if they "lend")
	Providers of deposit boxes
	Specialised financial institutions
	Cash handling firms
DNFBPs	*Accountants*
	Auditors
	Casinos
	Dealers in precious metals and stones
	Lawyers (including barristers, solicitors, and other legal professionals)
	Notaries
	Real estate agents (including licensed conveyancers)
	Trust and company service providers (including: company formation agents)
	All (Other) DNFBPs

Sector	Categories of institutions and firms
Other entities	*Advisors, including tax and financial*
	Bookmakers, betting, gaming & lotteries
	Motor vehicle retailers
	Boat charterers, sellers, and re-sellers
	Aircraft charterers, sellers, and re-sellers
	Art and antique dealers
	Auction houses
	Other dealers and traders in high value goods
	Pawnshops
	Travel Agents
	Convenience, grocery, liquor stores
	Laundromats, car washes, parking businesses
	Other cash intensive businesses
	Construction companies
	Customs agencies and brokers
	Mail and courier companies
	Hotels
	Restaurants and bars
	Mining, logging, and other extractive industry companies
	Other
Legal persons	*Bodies corporate*
	*Registered companies **
	*Public companies **
	*Companies that have issued bearer shares **
	*Companies owned or controlled by non-residents **
	*International or (foreign) business companies or corporations **
	*Other types of company **
	Foundations
	Anstalt
	Partnerships
	Associations
	Similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property
	All legal persons (other than companies) that are owned or controlled by non-residents including branches or offices of foreign legal persons authorised to operate in the

Sector	Categories of institutions and firms
	*jurisdiction **
Legal arrangements	*Express trusts (i.e., with a written deed of trust)*
	Fiducie
	Treuhand
	Fideicomiso
	Other similar legal arrangements
	*International Trusts**
	*All legal arrangements established or controlled by non-residents**
Non-profit organisations (NPOs)	*NPOs - registered or licensed*
	NPOs - not registered or licensed
	*All NPOs established or controlled by non-residents**

Table note
* These are memorandum items only as they should already appear in other categories.

ANNEX III. EXAMPLES OF NATIONAL-LEVEL ASSESSMENTS

This annex shares countries' efforts to assess ML/FT risks at the national level (whether focusing on threats, vulnerabilities, or both). These are presented as examples only. At the time of the publication of this guidance, the individual efforts had not been assessed for compliance with Recommendation 1; therefore, their presentation here should not be considered as an endorsement by FATF.

Australia

FATF Guidance on risk assessments – project group

Australian National Threat Assessment on Money Laundering 2011 (NTA)

Australia adopted a 'top-down' approach in 2011, producing the country's first National Threat Assessment (NTA). The NTA was a key element of the organised crime strategic framework the Australian Government adopted in 2009. The NTA involved only government agencies. AUSTRAC, the national FIU and AML/CFT regulator (*i.e.,* supervisor), led the project with primary input coming from five national government agencies (policy, revenue, law enforcement and border protection) and one state-based law enforcement intelligence agency. Incidental information came from a handful of national and state agencies on particular issues as required.

A two-tiered system was established to coordinate input and provide direction across agencies. A steering committee of senior officials was formed to provide guidance and governance to the assessment and resolve any issues that arose. The level below involved a working group of intelligence analysts, law enforcement officers and policy advisers to collect and analyse information, and work with the FIU on drafting the assessment. Once approved by the steering committee and the head of the FIU, the assessment was submitted to the heads of operational agencies in national government (comprising law enforcement, the FIU, border protection and regulatory agencies).

The NTA draws together information from across key government agencies to form a consolidated picture of the Australian money laundering environment. It is focused on the Australian environment and what Australian agencies and experts see as the current and emerging threats. Close attention is paid to money laundering associated with higher risk organised crime activity. It also examines high-risk countries that influence the Australian environment. International experience is drawn upon where required to amplify an aspect of the Australian situation, or to help address gaps in the Australian picture.

Information sources are primarily intelligence based. Current intelligence insights, operational cases, and expert views inform the discussion of current and projected money laundering activity. Limited statistical data, particularly the financial value tied to money laundering activity, meant the NTA is largely a qualitative threat assessment.

Threat matrix

The NTA modified the 'features' adopted in the FATF *Global Money Laundering and Terrorist Financing Threat Assessment* (GTA)[31], using terminology about channels, sectors and vulnerable individuals (industry insiders and PEPS) that would be readily understood by an Australian audience. Assessment of each area took into account:

- Government measures (law and regulation, law enforcement and regulatory activity, specialist intelligence work where relevant)
- Current intelligence picture
- Drivers and enablers (adopted from the GTA)
- Gaps in intelligence, information and measures
- Threat assessment with a three-year forecast where possible

To overcome the limitations faced in trying to apply conventional threat analysis (intent x capability = threat) to money laundering, a threat matrix (see Table 2 below) was customised for Australia's circumstances to rank relative levels of threat. It assessed threats and vulnerabilities in terms of:

- **Accessibility** or availability of services that might be misused for ML – scale from easy, moderate to difficult (the easier to access, the higher the threat)
- **Ease of use** – same scale as above
- **Deterrence** – scale of significant, limited to weaker (significant = measures reasonably effective at lowering threat of ML)
- **Detection** – scale of likely (detection of ML), limited to difficult (detection is unlikely due to intelligence gaps, opaque and complex services)
- **Criminal intent** to launder (a function of the above categories and assessments of current and emerging organised crime behaviour and trends)

Weightings for the scales used above were developed to produce rough scores of levels of threat, from undetermined to low, through to medium and high. Scoring was not adopted as a strict science, but rather as a starting point to stimulate expert discussion among the involved agencies. Threat scores were also used in conjunction with the analysis of each area, to test intelligence judgements and, vice versa, test the validity of the scoring system itself.

[31] FATF (2010).

Table 2. **Australian Threat Matrix**

Threat factors	Low threat	Medium threat	High threat
ACCESSIBILITY ***e.g.* accessibility and relative cost**	**Difficult** Difficult to access and/or may cost more than other options.	**Moderate** Reasonably accessible and/or a financially viable option.	**Easy** Widely accessible and available via a number of means and/or relatively low-cost.
EASE OF USE ***e.g.* knowledge and/or technical expertise and support required**	**Difficult** Requires more planning, knowledge and/or technical expertise than other options.	**Moderate** Requires moderate levels of planning, knowledge and/or technical expertise.	**Easy** Relatively easy to abuse; little planning, knowledge and/or technical expertise required compared to other options.
DETERRENCE ***e.g.* existence of AML and/or other barriers to abuse**	**Significant** Deterrence measures and controls exist and are reasonably effective at deterring money laundering.	**Limited** Deterrence measures and controls have some effect in deterring criminal abuse of the service.	**Weaker** There are limited or no measures and controls in place, or they are not working as intended.
DETECTION ***e.g.* ability for money laundering to be identified and reported to authorities**	**Likely** A range of money laundering methods is visible and likely to be detected.	**Limited** Some money laundering methods may be visible but limited reporting, high volumes of funds flows and/or effective evasion techniques limits detection.	**Difficult** Detection is difficult and there are few financial or other indicators of suspicious activity.
INTENT ***e.g.* perceived attractiveness of money laundering through this mechanism**	**Low** Perceived as relatively unattractive and/or insecure.	**Moderate** Perceived as moderately attractive and/or fairly secure.	**High** Perceived as attractive and/or secure.

High-risk countries[32]

To improve the capacity of Australian authorities to assess and weigh-up the ML threats/risks foreign countries pose to Australia, the NTA developed a high-risk country matrix. It essentially is a checklist of the main indicators and attributes which influence a country's risk profile, as a source, destination or conduit for laundered funds. A copy of the matrix table, sanitised with countries removed, is attached to this paper. It involved a larger set of indicators (listed below) than the

32 Even though the NTA is a threat assessment, the term 'high-risk countries' was used due to its commonplace usage in official circles.

threat matrix above. Many of the risk indicators are drawn from FATF guidance. Numerical weightings or scoring were not used with the matrix, but the format lends itself to such an approach if required.

For the sake of clarity, the NTA divided high-risk countries into two broad crime types: organised/transnational crime and offshore tax evasion. Although the boundary between these two categories is blurred and some countries appear in both groups, this approach helped to sift through a long list of countries. It also provided a sharper focus on the nature of illicit funds flows involving different countries, than would have been the case if they had all been lumped under the 'high-risk' tag.

High-risk country indicators

- Variable regulations, such as lax AML/CFT provisions, weak regulation of business registration, financial markets and foreign currency exchange
- Preferential tax regimes identified by the OECD
- Strong secrecy provisions in banking and finance
- High volume of non-bank international remittances
- Regional or global financial centres
- Free-trade or special economic zones
- Source countries for illicit commodities and services
- Transit countries for illicit commodities and services
- Low tax on foreign income
- Ability to easily create complex legal entities to hide beneficial ownership of assets
- Countries with perceived high-level corruption
- Countries embroiled in high-level internal or external conflict
- Patterns of evasion of exchange controls by legitimate businesses
- Limited asset forfeiture and seizure powers
- Weak law enforcement and border control capabilities
- Large parallel or black market economies
- Cash intensive economies
- Countries with no extradition treaty with Australia
- Jurisdictions that are either a place of residence for members of a criminal network or where members of a criminal network have strong familial or cultural ties, or both
- Jurisdictions where criminal entities can obtain dual nationality

Approach and lessons learnt

Since it was Australia's first NTA, the intention was to involve a core of key government agencies in laying the foundations upon which subsequent national assessments could build. Wider involvement from industry and other government bodies at the national and state/territory level is something to be considered for future assessments.

A key lesson from the first NTA is that any decision to involve more partners or stakeholders should be made on the basis of the value of data, intelligence and expertise they can commit to an assessment. Relevant expertise and a guaranteed commitment of resources (staff and time) are essential for the successful completion of such a large exercise. The 'hidden cost' in time and staff in consulting and coordinating many stakeholders should not be underestimated.

The NTA examines only money laundering and excludes terrorism financing threats. Differences between ML and TF, limited cases in the Australian context and difficulties in managing highly sensitive intelligence were all seen as likely to create added problems for a complex assessment that was first of its kind in Australia and largely exploratory. As with the decision to limit the number of agencies involved, the NTA was seen as paving the way to undertake a TF assessment in the future.

The NTA originally included, in line with the GTA framework, harms analysis for each area under examination. Harms were later omitted to avoid any conceptual confusion as to whether the NTA was a *threat* assessment (harms or consequences excluded) or a *risk* assessment (harms and consequences included). The more important reason for the omission was due to the lack of available evidence of ML harms in Australia, beyond sustaining continued and expanded criminal activity. Overseas experience of ML harms was largely seen as not directly relevant or provable in the Australian context.

The Netherlands

In 2005, a study was conducted titled: "The Amounts and Effects of Money Laundering"[33]. Its objective was to obtain better information on the amount, flows and effects of money laundering. The study was based on a quantitative method to estimate the amounts, flows and effects of money laundering. In addition, (extensive literature) research was carried out on definitions, typologies and growth effects. There was also an effort to identify forms of money laundering, typically existent in The Netherlands. The findings were mainly based on qualitative judgments but sometimes supported by quantitative data. The results of the study were used as input for policy formulation.

In 2011 a National Threat Assessment (NTA) was carried out in the Netherlands. The Ministry of Finance was leading the project and established a project plan which was submitted to and approved by the Financial Expertise Centre[34]. The exercise commenced by interviewing all relevant stakeholders, including for example: financial sector, supervisory authorities, research institutes

[33] Unger *et al.* (2006).

[34] The Financial Expertise Centre (FEC) is a partnership between authorities that have supervisory, control, prosecution or investigation tasks in the financial sector and was founded to strengthen the integrity of the sector. Authorities involved in the FEC are: Dutch Central Bank, Financial Markets Authority, Public Prosecutor, Tax Authorities, Intelligence Services, National Police, Ministry of Justice and Ministry of Finance.

and law enforcement. Based on the outcome of these interviews, the project team identified a list of mayor topics/issues and organised several workshops to discuss the selected items. Participants in these workshops where policymakers, supervisory authorities, prosecutors, police and tax authorities. As a result of this series of workshops three mayor topics where identified and these became subject of an in depth research. The project team analysed and described cases and trends/developments on these items and made recommendations for further work on these issues. Finally, the report has been presented to the Ministry of Finance and the Ministry of Justice with the objective to translate the outcome of the NTA into national policy measures. Relevant information resulting from this process has been published or made available to relevant non-public bodies, but the NTA itself remained a classified document.

In 2012 the National Police Services Agency (KLPD) conducted a National Threat Overview focused on money laundering. The method used by the KLPD was the following: again the research was commenced by a series of interviews with stakeholders. These interviews served as a basis for an in depth research in criminal files and data systems. This resulted in a description of several methods of money laundering, characterisation of persons involved and consequences for the Dutch society. Finally, the National Threat Overview is addressing some general developments concerning money laundering in the future.

Switzerland: Example of a risk assessment used as the basis for applying low-risk exemptions

Switzerland has developed a risk assessment process as a basis for applying low risk exemptions. A working group was established from September 2009 to January 2010, which was composed of experts from the banking, insurance and non-banking sectors, auditors, law enforcement authorities and the financial regulator. The working group identified low-risk products for which the exemptions could apply. This work resulted in the adoption of regulation which establishes an ongoing risk assessment process.

On the basis of the aforementioned regulation, a committee of experts, established by FINMA, can authorise exemptions from CDD measures for customer relationships at the request of SROs or financial intermediaries if there is a proven low risk for money laundering. In order to get a decision from FINMA allowing a financial intermediary to benefit from an exemption, the requestor has to provide all elements necessary for FINMA to take this decision. FINMA then verifies if the regulatory conditions for an exemption are met, and in particular if the low risk is given on a case-by-case basis. To come to a decision, FINMA analyses every request separately and in detail. Different criteria are taken into consideration. FINMA examines whether the FATF has already considered the activity under the risk aspect. It examines if similar cases have already been subject to criminal or other enforcement measures. Finally, FINMA decides if the risk is low in the concrete case, but also if it will remain low if the circumstances would slightly change. Consideration is given to product, services, transactions as well as customer risk and to the legal environment, as well as to every other relevant characteristic of the activity, in order to decide whether the risk is low. FINMA has the legal obligation to publish its practice.

United States

In 2005, the United States initiated its first multi-agency money laundering threat assessment. Quantitative inputs included prosecution data from federal law enforcement agencies and suspicious transaction reporting via the financial intelligence unit. Qualitative inputs came from law enforcement and regulatory case studies with private sector reporting.

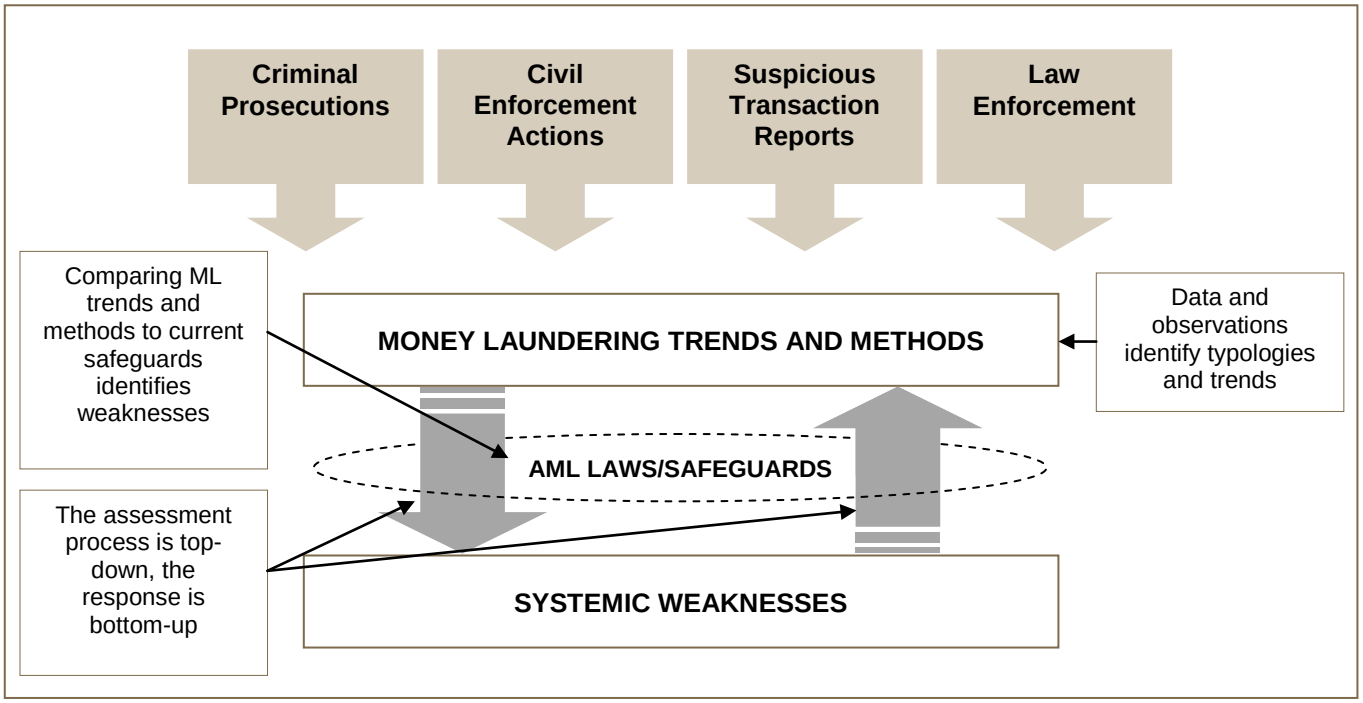
The 2005 *U.S. Money Laundering Threat Assessment*[35] was divided into the following sections: banking, money services businesses, (*i.e.*, money transmitters, cheque cashers, currency exchangers, money orders and stored value cards); online payment systems; informal value transfer systems; bulk cash smuggling; trade-based money laundering; insurance companies; shell companies and trusts; and casinos.

The project team made assumptions and observations about vulnerable sectors using the available information, considered whether adequate safeguards were in place to address the identified vulnerabilities and made a subjective determination about the residual threat.

This was a multi-agency process, including offices and agencies under the US Departments of Homeland Security, Justice and Treasury. Also participating was the Board of Governors of the Federal Reserve System and the United States Postal Inspection Service.

The available information was synthesised to form a qualitative assessment, which included, to the extent possible, the relative effectiveness of AML safeguards. In some cases, data was available to support subjective judgments regarding effectiveness (see Figure 5). Otherwise, the determinations were the result of broad intergovernmental discussion and analysis.

Figure 5. **Flow chart depicting US money laundering assessment and strategy formation process**



35 Money Laundering Threat Assessment Working Group (U.S. Department of the Treasury, *et al.*) (2005).

ANNEX IV. SPECIFIC RISK ASSESSMENT METHODOLOGIES

The International Monetary Fund Staffs' ML/FT National Risk Assessment Methodology:
www.fatf-gafi.org/media/fatf/documents/reports/Risk_Assessment_IMF.pdf

The World Bank Risk Assessment Methodology
www.fatf-gafi.org/media/fatf/documents/reports/Risk_Assessment_World_Bank.pdf

BIBLIOGRAPHY

Relevant FATF material (all available at: www.fatf-gafi.org)

FATF (2012), *The FATF Forty Recommendations*, FATF, Paris.

FATF (2010), *Global Money Laundering and Terrorist Financing Threat Assessment*, FATF, Paris.

FATF (2008), *Money Laundering and Terrorist Financing Risk Assessment Strategies*, FATF, Paris.

FATF, (2007), *Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*, FATF, Paris.

Country-level assessments of interest (available on line)

Australia:

AUSTRAC (2011), *Money laundering in Australia 2011*, Sydney, www.austrac.gov.au/files/money_laundering_in_australia_2011.pdf

Netherlands:

Unger *et al.* (2006), *The Amounts and the Effects of Money Laundering, Report for the Ministry of Finance*, Amsterdam, www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2006/02/16/onderzoeksrapport-the-amounts-and-the-effects-of-money-laundering/witwassen-in-nederland-onderzoek-naar-criminele-geldstromen.pdf

New Zealand:

New Zealand Police (2010), *National Risk Assessment 2010*, Wellington, www.justice.govt.nz/policy/criminal-justice/aml-cft/publications-and-consultation/20110308-NRA-2010-Primary-Document-FINAL.pdf

New Zealand Department of Internal Affairs (2011), *Internal Affairs AML / CFT Sector Risk Assessment,* Wellington, www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf/$file/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf.

New Zealand Securities Commission (2011), *Sector Risk Assessment*, Wellington, www.fma.govt.nz/media/186534/aml-cft-sector-risk-assessment.pdf.

Reserve Bank of New Zealand (2011), *Sector Risk Assessment*, Wellington, www.rbnz.govt.nz/aml/4345201.pdf.

United States:

Money Laundering Threat Assessment Working Group (U.S. Department of the Treasury, *et al.*) (2005), *U.S. Money Laundering Threat Assessment*, U.S. Department of the Treasury, Washington, DC, www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf

Other material

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2004), *Enterprise Risk Management – Integrated Framework*, COSO, website: www.coso.org/erm-integratedframework.htm.

European Network and Information Security Agency (ENISA) (2006), Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment Methods and Tools, Heraklion [Greece], website: www.enisa.europa.eu/activities/risk-management.

EUROPOL (2011), *Organised Crime Threat Assessment*, Europol, The Hague, www.europol.europa.eu/sites/default/files/publications/octa_2011_1.pdf.

The Institute of Risk Management et al. (2002), *A Risk Management Standard*, [United Kingdom], www.theirm.org/publications/PUstandard.html.

International Organisation for Standardisation (ISO) (2009a), *Risk Management – Principles and Guidelines* (ISO 31000:2009), ISO, Geneva, website: www.iso.org.

ISO (2009b), *Risk Management – Risk Assessment Techniques* (ISO 31010:2009), ISO, Geneva, website: www.iso.org.

ISO (2009c), *Risk Management – Vocabulary* (ISO Guide 73:2009), ISO, Geneva, website: www.iso.org.

Organisation for Security and Co-operation in Europe (OSCE) (2012), *OSCE Handbook on Data Collection in Support of Money Laundering and Terrorism Financing National Risk Assessment*, Vienna, www.osce.org/eea/96398.

Standards Australia and Standards New Zealand (2009), *Risk Management – Principles and Guidelines* (AS/NZS ISO 31000:2009), SAI Global, website: www.infostore.saiglobal.com/store.

Treasury Board of Canada (2001), *Integrated Risk Management Framework*, Ottawa, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text.

United Nations Office on Drugs and Crime (UNODC) (2010), *Guidance on the preparation and use of serious and organised crime threat assessments* ["The SOCTA Handbook"], UNODC, Vienna, www.unodc.org/documents/afghanistan/Organized_Crime/SOCTA_Manual_2010.pdf.

U.S. Department of Homeland Security (2010), *DHS Risk Lexicon – 2010 Edition*, Washington DC, www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.