

The New FATF Methodology

Malta, July 2015

Assessment Timeframes

- AML/CFT and the upcoming IMF Financial Sector Assessment Program – Dates TBD
 - Likely to cover only some Recommendations – targeted review?
 - May but may not involve an onsite visit
 - No ratings
 - No separate TC and Effectiveness assessment – more of a thematic approach
 - Structure does not follow FATF Methodology
- The next full AML/CFT assessment by CoE Moneyval – sometime 2018
 - Full assessment - will cover both technical compliance and effectiveness
 - Large team visiting Malta for approximately two weeks
 - Focus exclusively on AML/CFT
 - Separate ratings for effectiveness and technical compliance
 - Follows FATF Methodology

Previous FATF Methodology

- 40 Recommendations on Anti-Money Laundering (AML), 9 Special Recommendations on Combating Financing of Terrorism (CFT)
- For each Recommendation, write up on technical compliance (TC) followed by an analysis and findings on effectiveness
- 49 composite ratings for technical compliance and effectiveness

Process under Old Methodology

- Preparations by country involved filling out a detailed questionnaire
- Assessors prepared first draft of the entire report onsite or after onsite visit
- Discussion onsite focused largely on TC issues

New FATF Methodology

- 40 Recommendations in total, including CFT aspects
- Recommendations focused exclusively on TC – legal requirements and powers, processes, institutional structures, etc.
- IN ADDITION, 11 Immediate Outcomes (IOs) now define how to measure effectiveness of the AML/CFT system as a whole
- Separate sections of the report as well as separate ratings for TC and IO assessments

Process under New Methodology

- Authorities to provide update on all TC aspects compared to last MER – not a full questionnaire! PLUS description of how IOs are met
- Most of the TC analysis work is done by the assessors well in advance of the onsite mission and based on a desk review
- Draft TC assessment report provided to the authorities beforehand
- Idea is that the TC component is completed before the onsite visit
- Onsite visit will focus almost exclusively on effectiveness issues and the IOs

Technical Compliance

- Requirements addressing legal, regulatory or procedural issues
- Often merely a question of “yes” or “no”
- Separate rating for each Recommendation
- Information is drawn from previous MER, except where laws and requirements were changed
- Write up is much shorter than in previous rounds, less descriptive, aims to avoid overlap with and will often refer to last MER
- Some of the TC requirements were changed, removed or added, but lots of them stayed the same, some Recs are new
- Main difference is that there is now much greater emphasis on TC requirements to be risk based – example CDD

40 Recommendations

- 1 and 2: *National Risk Assessment and Coordination*
- 3 to 5: ML and FT offenses and Confiscation
- 6 and 7: Targeted financial sanctions FT and WMDs (UNSCRs)
- 8: Transparency of NPOs
- 9 -16: Preventive Measures and Additional Measures for Certain Customers and Activities
- 17 - 19: Third party reliance, internal controls and high risk countries
- 20 - 21: STR reporting
- 22 - 23: DNFBPs
- 24 - 25: Transparency of legal entities and legal arrangements
- 26 - 28: Supervision
- 29 - 32: LEAs, FIU and Cash Couriers
- 33 - 35: Statistics and Sanctions
- 36 - 40: International Cooperation and Extradition

National Risk Assessment

- Specific Recommendation on this issue now (R 1)
- Requirement is twofold:
 - For countries to carry out a national risk assessment, covering all sectors and aspects
 - For FIs and DNFBPs to carry out an institutional risk assessment covering product, delivery channel, customer and geographic risks
 - TWO SEPARATE OBLIGATIONS THAT REQUIRE SEPARATE ACTION ITEMS
 - Idea is to ensure that resources allocated according to the risks, that CDD and other preventive measures are applied in line with the risks, that policies are framed in line with the risks posed etc.
 - In sum: compliance is tied to a greater number of requirements but we have more flexibility in how we implement these requirements

Effectiveness

The extent to which each of the 11 Immediate Outcomes is achieved

- How well is the country mitigating the risks of ML and FT?
- Does the AML/CFT system work in practice?
- Outcomes not outputs – not statistics and numbers but the difference made by the outputs matters!
- Judged by experience, not tick-box approach
- Not the same as “efficiency”

Links between TC and Effectiveness

- A high level of technical compliance *does not* automatically lead to a high level of effectiveness.

BUT

- It is unlikely that country with low level of technical compliance with the relevant Recommendations will be effective.
 - May be exceptional circumstances where low level of technical compliance can be consistent with a certain level of effectiveness.
 - If so, assessors must fully justify their decision, explaining in detail the basis and the specific reasons for their conclusions on effectiveness.

11 Immediate Outcomes

- IO 1: Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.
- IO2: International cooperation delivers information, financial intelligence, and evidence, and facilitates action against criminals and their assets.
- *IO 3: Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks.*
- *IO 4: Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.*
- IO 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.

11 Immediate Outcomes

- IO 6: Financial intelligence and all other relevant information are used appropriately by competent authorities for money laundering and terrorist financing investigations.
- IO 7: Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.
- IO 8: Proceeds and instrumentalities of crime are confiscated.
- IO 9: Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.
- IO 10: Terrorists, terrorist organizations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.
- IO 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.

Effectiveness

- Is now the absolute focus of every assessment
- Before, effectiveness was part of assessment of each component – FIU effective, LEAs effective, PPO effective etc.?
- Now, it's the interlinkages that are subject to assessment – is the system as a whole effective, are the linkages between the various institutions and components working?
- Effectiveness assessment mostly done during the onsite visit with some preparatory work done beforehand
- Several rounds of discussions subsequent to the onsite visit



Coffee Break

“Old” Recommendation 5 criteria

- Financial institutions should be required to identify the customer (whether permanent or occasional, and whether natural or legal persons or legal arrangements) and verify that customer’s identity using reliable, independent source documents, data or information (identification data).
- *For customers that are legal persons or legal arrangements, the financial institution should be required to:*
 - *(a)* verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person; and*
 - *(b) verify the legal status of the legal person or legal arrangement, e.g. by obtaining proof of incorporation or similar evidence of establishment or existence, and obtain information concerning the customer’s name, the names of trustees (for trusts), legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement.*
- *Financial institutions should be required to identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is.*

New Recommendation 10

- *For customers that are legal persons³¹, 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) who ultimately has a controlling ownership interest³³ in a legal person; and*
 - *(b) to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and*
 - *(c) where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.*
- *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 beneficiaries³⁴, 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.*

PLUS Effectiveness of Preventive Measures

Immediate Outcome 4

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

Core Issues

- How well do FIs and DNFBPs understand their risks and obligations?
- How well do they apply mitigating measures?
- How well do they apply CDD and record-keeping? Is business refused?
- How well are specific measures applied? (e.g. PEPs, correspondent banking, wire transfers rules, financial sanctions)
- How well do they meet their reporting obligations?
- How well do they apply internal controls?

Examples of Information that Support Conclusions on Core Issues

- 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*).
- Information (including trends) relating to risks and general levels of compliance (e.g., *internal AML/CFT policies, procedures and programs, trends and typologies reports*).
- Examples of compliance failures (e.g., *sanitized cases; typologies on the misuse of financial institutions and DNFBPs*).
- 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*).
- 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 analyze the suspicious transaction before filing an STR*).

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

- What are the measures in place to identify and deal with higher (and where relevant, lower) risk customers, business relationships, transactions, products and countries?
- 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?
- 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?
- How well do financial institutions and groups, and DNFBPs ensure adequate access to information by the AML/CFT compliance function?
- 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?

Examples of Specific Factors that could support the conclusions on Core Issues (2)

- 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?
- 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?
- How well are financial institutions and DNFBPs documenting their ML/TF risk assessments, and keeping them up to date?
- 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?
- How well is feedback provided to assist financial institutions and DNFBPs in detecting and reporting suspicious transactions?
- To what extent is there reliance on third parties for the CDD process and how well are the controls applied?

“Old” Recommendation 23

- Countries should ensure that financial institutions are subject to adequate AML/CFT regulation and supervision and are effectively implementing the FATF Recommendations.
- Countries should ensure that a designated competent authority or authorities has/have responsibility for ensuring that financial institutions adequately comply with the requirements to combat money laundering and terrorist financing.
- Supervisors or other competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function, including in the executive or supervisory boards, councils, etc. in a financial institution.
- Directors and senior management of financial institutions subject to the Core Principles should be evaluated on the basis of “fit and proper” criteria including those relating to expertise and integrity.
- *For financial institutions that are subject to the Core Principles the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes, except where specific criteria address the same issue in this Methodology.*
- *Financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector i.e. if there is a proven low risk then the required measures may be less.*

New Recommendation

- Countries should designate one or more supervisors that have responsibility for regulating and supervising (or monitoring) financial institutions' compliance with the AML/CFT requirements.
- **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.
- Financial institutions should be subject to:
 - (a) *for core principles institutions* - regulation and supervision in line with the core principles, where relevant for AML/CFT, including the application of consolidated group supervision for AML/CFT purposes.
 - (b) *for all other financial institutions* - regulation and supervision or monitoring, having regard to the ML/TF risks in that sector.
- **The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions or groups should be determined on the basis of:**
 - (a) **the ML/TF risks and the policies, internal controls and procedures associated with the institution or group, as identified by the supervisor's assessment of the institution's or group's risk profile;**
 - (b) **the ML/TF risks present in the country; and**
 - (c) **the characteristics of the financial institutions or groups, in particular the diversity and number of financial institutions and the degree of discretion allowed to them under the risk-based approach.**
- **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.**

PLUS Effectiveness of Supervision

Immediate Outcome 3

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

Core Issues

- 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?
- 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?

IO 3 Core Issues (2)

- 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?
- To what extent are remedial actions and/or effective, proportionate and dissuasive sanctions applied in practice?
- To what extent are supervisors able to demonstrate that their actions have an effect on compliance by financial institutions and DNFBPs?
- How well do the supervisors promote a clear understanding by financial institutions and DNFBPs of their AML/CFT obligations and ML/TF risks?

Examples of Information that Support Conclusions on Core Issues

- 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*).
- 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 practices, thematic studies; annual reports*).
- Information on supervisory engagement with the industry, the FIU and other competent authorities on AML/CFT issues (e.g., *providing guidance and training, organizing meetings or promoting interactions with financial institutions and DNFBPs*).
- Information on supervision (e.g., *frequency, scope and nature of monitoring and inspections (onsite 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*).

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

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

Examples of Specific Factors that could support the conclusions on Core Issues (2)

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

Analysis Process

Conclusions based on an overall understanding of the degree to which the country is achieving the outcome.

- Assessment report will identify:
 - Strengths and good practices
 - Variations in effectiveness
 - Problems and weaknesses

“How well...?”

“To what extent...?”

- What level of performance do we expect?
 - On the basis of comparisons
 - On the basis of risk and materiality
 - On the basis of the country’s situation
 - Interpretation vs Explanation

Information Source

- Country is the primary source of information
 - Key sources listed in “examples of information”.
- Can supplement this with other credible, reliable sources
 - International organizations
 - Major authoritative publications
 - Referenced / Checked with other sources

Questions?





THANK YOU!

Gabriele Dunker

Consultant

Gabriele.dunker@gmail.com