Auditing Money Laundering and Terrorist Financing Risks of MENA Institutions: The Trials and Tribulations

Angeli Pereira
October 2018
Disclaimer:

Angeli Pereira is currently an Associate Director, AML/CFT Supervision at the Qatar Financial Centre Regulatory Authority. With the exception of references and extracts from publicly sourced documents, the content and views expressed in this paper are the author’s and should not be interpreted as representing the views, opinions, or policies of the Regulatory Authority or any past employer.
Contents
1. Executive Summary ................................................................. 4
2. Objectives ........................................................................ 5
3. Background ........................................................................ 5
4. Importance of Risk Assessments ........................................... 6
   4.1. For Regulators ................................................................. 6
   4.2. For the Firm’s Internal Stakeholders ................................. 6
   4.3. For Correspondent Banking Relationships ........................ 7
5. Mandatory Obligation to Conduct an Independent Review/Audit ....... 7
6. AML Failures and Their Consequences ...................................... 7
   6.1. AML Cases: International and Regional ............................ 7
   6.2. Main Lessons Learned From the Above Cases ..................... 9
7. Business Risk Assessment .......................................................... 9
   7.1. Identification of the Inherent Risks ..................................... 10
   7.2. Control Environment Factors ............................................. 10
   7.3. Residual Risk .................................................................. 11
8. A Threat Assessment Methodology .............................................. 12
9. Risk Profiling of Business Relationships ..................................... 12
10. Skillset Required for Auditing ML/TF Risks ................................. 13
13. Key Takeaways and Conclusion .............................................. 18
14. Glossary ........................................................................... 19
15. References ........................................................................ 20
16. Appendix A – An Audit Checklist for Risk Assessments .............. 22
**Executive Summary**

This paper has been structured in a manner to give a broad yet simple understanding of risk assessment in terms of the main pillars, processes, and other considerations; and to delve deeper into the nuances of auditing a risk assessment. It is often observed that large global firms are better placed with risk assessments, in terms of structure, process, and resources. It is the smaller firms that face challenges, in terms of how to conduct a risk assessment, where to begin, what direction to take, whether to incorporate a scoring mechanism or not, and so forth.

While the paper focuses on the Middle East and North Africa (MENA) region, many principles and issues apply across all regions and are therefore relevant to readers in other parts of the world. This paper is conceptualized to improve the industry’s understanding of risk assessments and to highlight key issues from an auditor’s perspective. It also contains a comprehensive list of reference sources, should the audience wish to further expand its understanding.

It is the author’s intention that this paper be able to assist AML practitioners—such as MLROs, compliance officers, risk managers, and AML auditors—irrespective of the size of the firm. AML practitioners will benefit from the level of detail on how to conduct an ML/TF risk assessment, as best practices are described throughout. This, in addition to the provided regulatory expectations, will assist readers in understanding the risk assessment process.

For AML auditors, this paper contains a practical guide as to what to look for and how to plan. While this paper cannot cover the intrinsic details related to all sectors, it gives broad indicators. As a tool, an audit checklist is appended.

It is important to note that like firms, most regulators adopt a risk-based approach to regulation and supervision that includes risk-rating their regulated population of firms. The risk rating may include a consolidated view of all types of risks a firm is exposed to, such as prudential, liquidity, credit, market, and AML/CFT. Individual risk ratings are derived for each firm, and that places them on sectoral heat maps—such as for banks, money service businesses, insurance, advisory, investment managers, and DNFBPs, etc.—and further aggregates into a consolidated heat map to represent the regulated population on a “dashboard.” Corresponding to the risk rating of firms, a supervisory cycle is set that dictates the level of supervisory engagement. The higher the risk, the greater the supervisory engagement.

Due to the risk-based approach to regulation, some regulators have made it a mandatory rule requirement for a firm’s ML/TF risk assessment to be audited at frequent intervals. Internal audit is the third line of defense and an important partner of a regulator, with both parties working toward sound compliance and regulation. Audit reports are reviewed, scrutinized, and actioned by regulators. When auditors fail to raise red flags and recommendations in their report, it becomes a point of concern resulting in enhanced supervision.

Fundamental to the success of a risk assessment is a good understanding of the risk factors of the relevant financial sector, industry, and segment. While the risk assessment is the responsibility of the AML or risk management department, or
perhaps the individual line of business, the role of the auditor is integral in the validation of the ML/TF risks identified and the mitigations in place.

**Objectives**
The paper intends to provide:

- An understanding of the importance of a risk assessment;
- A practical approach to risk assessment;
- Regulatory expectations and how to achieve them;
- The nuances of auditing a risk assessment, what and where to look; and
- An enhanced ability among auditors to identify ML/TF risks and the control gaps.

**Background**

**FATF Recommendation 1**:

"Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions. Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks."

FATF Recommendation 1 addresses the macro and micro requirement to identify ML/TF risks, at the national and firm levels. Countries are required to conduct a “national risk assessment” of the ML/TF risks posed to them by various sectors and to allocate sufficient resources into the mitigation of the risks identified. This macro-level requirement then cascades into the micro level, where firms have to identify their ML/TF risks and mitigate them effectively. Firms must develop a program against ML and TF and are expected to assess the ML/TF risk(s) they may reasonably face in conducting business, with regard to their business (size, nature, and complexity).

**As per the Basel Committee on Banking Supervision (BCBS)**:

"Sound risk management requires the identification and analysis of ML/FT risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks. In conducting a

---

1 FATF Recommendations 2012
2 BCBS’s ‘Sound Management of Risks related to Money Laundering and Financing of Terrorism’.
A comprehensive risk assessment to evaluate ML/FT risks, a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied.”

Firms are expected to demonstrate that their risk-based policies, procedures, systems, and controls are suitable to their particular businesses (with regard to their size, nature, and complexity) and are consistent with prudent and good practice. A well-reasoned and effective risk-based approach relevant to a firm’s business and circumstances should assist the firm in managing any ML/TF risks. Firms are encouraged to periodically review and evaluate their risk management framework, to ensure that it is effective, and to identify improvement opportunities that may arise.

**Importance of Risk Assessments**

**For Regulators**
Regulatory obligations must be adhered to, and that includes the need to conduct a risk assessment. Some regulators make the firm’s business risk assessment a mandatory submission. If the risk assessment falls short of regulatory expectations, it could lead to one or more of the following:

- The risk assessment may be rejected as being deficient, and the firm may be asked to re-conduct the risk assessment.
- A regulatory visit may be scheduled that targets a review of the risk assessment process.
- Private warning letters or public censures.
- Sanctions (referring to AML Failures and Their Consequences) in more stringent cases, such as when an enforcement investigation concludes that the firm was negligent in identifying and mitigating the ML/TF risks. This could also be detrimental for the auditor who has performed an audit on the risk assessment and who has failed to report on issues or breaches in his audit report to the firm’s senior management and regulator.

**For the Firm’s Internal Stakeholders**
The risk assessment results must be communicated to individual business divisions, senior management, the audit and risk committee, and the Board, etc. to assist in the following:

- To fix gaps identified in AML/CFT policies, procedures, systems, and controls.
- To compare current and previous risk assessments to determine if the risk rating has increased, decreased or remained constant.
- Senior management must determine if the risk rating is within the risk appetite (and risk tolerance) of the firm, while keeping in mind its strategic goals.
- Consider whether to initiate a targeted audit of any high-risk area identified.
- Decide on the frequency of independent reviews or audits—a risk-based audit plan.
- Communicate with regulators on the key issues identified during the risk assessment and action plans to remediate the issues.
For Correspondent Banking Relationships
A correspondent bank will seek to understand the risk rating of a respondent bank. This is an important factor in making a business decision as to whether to commence the relationship (or not) and, further, whether to maintain it.

In the perilous times of de-risking, firms must make sure that they adhere to the correspondent bank’s requirements, including the need to conduct an adequate ML/TF risk assessment.

Mandatory Obligation to Conduct an Independent Review/Audit
Regulators, including those in the MENA region, such as the QFCRA\(^3\) and the DFSA,\(^4\) have made independent review/audit a mandatory rule obligation, which must include a review of the firm’s program against money laundering and terrorist financing. This includes a review or assessment, including testing of the firm’s compliance with its AML/CFT policies, procedures, systems, and controls.

This reiterates the reliance placed by regulators on the independent review/audit of the firm’s AML/CFT program.

AML Failures and Their Consequences
Enforcement action by regulators worldwide has been gaining traction, with the severity of cases and the monetary aspect of penalties increasing steadily. While in the past there have been fewer publicly known enforcement cases in the MENA region, there appears to be an upward trend in the initiation of cases, particularly with AML/CFT. Due to regional sensitivities, at times, these are limited to private warnings instead of public censures.

AML Cases: International and Regional
The following are some cases selected from the international as well as regional area to highlight the importance of AML compliance, the consequences of failures in the AML/CFT program, and the overarching importance of auditing the AML/CFT framework of the firm.

In the Wachovia\(^5\) case, the AML program was deficient in three of the four core elements, including the failure to implement an effective independent audit function for testing with respect to the BSA, particularly the suspicious activity reporting requirements. A civil money penalty of US$110 million was imposed.

In the case of Pacific National Bank,\(^6\) in addition to other failings, the scope and frequency of independent testing for compliance with the BSA was not conducted in

---

\(^3\) QFCRA’s Anti-Money Laundering and Combating Terrorist Financing Rules 2010 (AML/CFTR)
\(^4\) DFSA’s Rulebook - Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module
\(^5\) United States of America Department if the Treasury Financial Crimes Enforcement Network against Wachovia Bank – Assessment of Civil Money Penalty -
\(^6\) United States of America Department of the Treasury Financial Crimes Enforcement Network against Pacific National Bank -
a manner that allowed for timely identification and correction of violations. Further, the bank did not adequately conduct periodic enterprise-wide risk assessments of the entire bank’s exposure to ML. A civil money penalty of US$7 million was imposed.

In the case of Ocean Bank, FinCEN had determined that the independent testing for compliance with the BSA was ineffective and failed to ensure compliance. The bank did not implement an effective independent audit function in terms of scope and frequency to manage the risk of ML and compliance with the BSA. A civil money penalty of US$10.9 million was imposed.

In the case of HSBC, the U.S. authorities imposed a fine of US$1.9 billion due to AML and Sanctions violations.

In the case of Deutsche Bank AG Dubai (DIFC) Branch, the DFSA issued a decision notice to fine the bank US$8.4 million for breaches on client take-on and AML rules.

More recently, Standard Chartered Bank, Singapore Branch was fined S$5.2 million and S$1.2 million on Standard Chartered Trust (Singapore) Limited (SCTS) by the Monetary Association of Singapore for breaches of its anti-money laundering and countering the financing of terrorism (AML/CFT) requirements.

Industrial & Commercial Bank of China (“ICBC”), the Board of Governors of the U.S. Federal Reserve, and ICBC entered into a consent cease-and-desist order for significant deficiencies in the branch’s risk management and compliance with applicable federal and state laws, rules, and regulations relating to AML compliance. Included in the actionable items was the need for ICBC to revise its internal audit program for the branch.

Following an investigation into the affairs of Guardian Wealth Management Qatar, the QFCRA identified systemic failures in the firm’s implementation of its AML/CFT policy, procedures, systems, and controls (PPSC). A financial penalty of US$987,000 was imposed for regulatory contraventions in addition to paying for costs and expenses of the investigation.

---

9 DFSA and Deutsche Bank AG Dubai (DIFC) Branch - Decision Notice - https://www.dfsa.ae/Documents/Regulatory%20Actions%202015/DBDIFC%20Decision%20Notice%2029032015%20for%20publication.pdf
11 S$ - Singaporean dollars
Main Lessons Learned From the Above Cases

1. Firms fail to conduct risk assessments entirely or conduct risk assessments that do not appropriately address the ML/TF risks of the firm, which in most jurisdictions is treated as a regulatory contravention.

2. An AML/CFT program must consist of well-documented policies and procedures to establish an effective control environment, the absence of which exposes the firm to ML/TF risks.

3. A well-resourced AML function and an independent audit team is critical. Firms must implement a risk-based audit program that covers appropriate areas of the business.

4. The need for audit to conduct a “deep dive” into detecting violations and systemic issues

Business Risk Assessment

A firm must be able to demonstrate that it has considered the exposure of its business to ML/TF risks. An ML/TF risk assessment is a product or process based on a methodology, agreed upon by those parties involved, that attempts to identify, analyze, 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.

The Business Risk Assessment\(^{14}\) must be documented, receive senior management’s approval, and be reviewed at periodic intervals. It is important for firms to establish and document their risk appetite, which defines the type, level, and extent of risks a firm is willing to expose itself to for the furtherance of its business activities. Senior management’s involvement and sign-off is an integral part of the process, as this could have an impact on the profitability and/or regulatory obligations of a firm.

The key purpose of an ML/TF risk assessment is to drive improvements in ML/TF risk management through identifying the general and specific ML/TF risks a firm is facing, determining how these risks are mitigated by a firm’s AML/CFT program controls, and establishing the residual risk that remains for the firm.

At a minimum, the risk assessment must be reviewed annually. Should there be a trigger event, such as new business or a new product, changes in the customer base, or transactions with higher risk countries, etc., the risk assessment must be conducted again. If it is feasible, the risk assessment may be conducted for the targeted area that has undergone changes, and then integrated into the broader risk assessment.

\(^{14}\) Some content of the business risk assessment has been sourced from the Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption and the QFCRA’s guidance on the Risk Based Approach, the hyperlinks to these documents have been provided under ‘References.’
The main pillars of a risk assessment are the identification of the inherent risks, evaluation of the control environment, and the determination of a residual risk rating, i.e., the firm’s AML/CFT risk rating, as explained below.

**Identification of the Inherent Risks**

Inherent risks represent the exposure to ML/TF and other financial crime risks, such as sanctions, bribery, and corruption, before assessing and applying the controls. At a minimum, the firm must identify the four risk factors as highlighted below. Additional risk factors specific to the firm’s nature, scale, and complexity may also be included such as reputation risk, regulatory risk, etc. All risks must be clearly documented and reviewed at regular intervals.

The illustration below identifies the four main risk factors—customer, product, interface, and jurisdiction—which should be based on a threat assessment methodology.

**Control Environment Factors**

Subsequent to identifying the inherent risks, a firm’s AML/CFT program (AML/CFT policies, procedures, systems, and controls) must be evaluated and mapped against the inherent risks.

Firms must have appropriate senior management oversight of ML/TF risks and a dedicated MLRO, deputy MLRO, and other staff dedicated to AML/CFT obligations and monitoring. Larger firms will need a fully dedicated AML/CFT unit. Staff are to be screened and trained with the overarching need for a strong AML/CFT culture with a top-down approach.

Firms should have particular focus on the key requirements of the relevant rules and legislations that constitute the building blocks for developing and implementing the program.
The following illustration contains some of the important components of the control environment.

**Residual Risk**
Once both the inherent risk and the effectiveness of the internal control environment have been considered, the residual risk can be determined. Residual risk is the risk that remains after controls are applied to the inherent risk. In effect, it is the score derived after deducting the control score from the inherent risk score.
A Threat Assessment Methodology

Firms are required to conduct their risk assessment based on a threat assessment methodology to enable the firm to identify any changes in these risks, including risks posed by new products and services or new or developing technologies. A firm may consider that frequent reassessments are appropriate in some cases (e.g., for a dynamic, growing business) and less frequent in other cases (e.g., an established business with stable products and services), and internal and external trigger events should always be considered when scheduling reassessments.

A threat assessment methodology is a methodology to identify and assess the threats a firm faces in the environment in which it operates. It is important to consider and record the threats applicable to the firm, its business model, and the environment in which it operates. This enables the firm and its stakeholders to understand what risks and actions are required to be taken to mitigate these risks.

Risk Profiling of Business Relationships

A common point of confusion arises in the understanding of the customers’ risk rating vs. the firm’s risk rating. Some firms, mistakenly, use these terms interchangeably. Firms must be cognizant of the need of having both: A firm-wide ML/TF risk assessment provides the final outcome as to the ML/TF risk rating of the firm, which in simple terms
is a macro view of the ML/TF risks. Risk profiling of the customers is a micro view of individual ML/TF risks associated with a customer.

The purpose of risk-profiling a business relationship is to provide the firm with a clear understanding of the customer business relationship and the resulting level of CDD measures and ongoing monitoring required for the business relationship.

At a minimum, firms must consider the following four key risk factors in developing the risk profile of a business relationship with a customer:

1. Customer risk;
2. Product/Service risk;
3. Interface risk; and
4. Jurisdiction risk.

The total consideration of all of the risk factors combines to produce the risk profile of the business relationship, and that risk profile must be considered in deciding the extent of the CDD measures and ongoing monitoring to be conducted for the customer.

**Skillset Required for Auditing ML/TF Risks**

For smaller firms that do not have a dedicated audit team, some regulators permit an MLRO of the group entity or an external consultancy to conduct the audit. Whether the auditor is internal or external, the minimum expectations are that the individual performing the audit has the requisite skills, knowledge, and experience to perform the audit. Apart from this, it is imperative that such an individual be “independent” of the work being audited. As an example, an audit report provided by the MLRO of a group entity will not be accepted by a regulator if the MLRO covered an interim period of AML/CFT obligations for the firm, as the “independence” requirement would be considered compromised.

It is recommended that an auditor attain an AML/CFT qualification to fulfil the knowledge criteria.

**A Differentiated Approach to AML/CFT Audits**

Auditors must be cognizant of the “subjectivity” aspect while auditing AML/CFT. While “objectivity” is the crux of most non AML/CFT audits, the element of subjectivity—i.e., an opinion or a perspective—must be factored in. As an example, financial auditors base their findings and final grading on “facts and figures,” which is distinctly objective. An AML auditor is expected to combine both aspects—objectivity and subjectivity—in the auditor’s findings.

**Challenges of Auditing ML/TF Risks: MENA and Global**

The MENA region is in a constant state of dynamism—politically, socially, and economically. Rapid changes in the region have significant consequences on the business of a firm, and this, in turn, impacts the operating environment. The size of a firm may not, by itself, be indicative of the extent to which it is exposed to ML/TF risk; firms that are relatively small can nevertheless pose a high ML/TF risk to themselves,
the rest of the regulated population, and the country’s financial system. In most instances, global firms are better equipped with auditing resources due to the existence of a broader base of expertise available within their group of firms.

For convenience, firms have been bucketed into two broad categories—MENA firms and global firms—to highlight the challenges faced in the two categories.

**MENA Region Firms**

A good starting point for auditors is to be aware of the typologies prevalent in that particular country and the region. Due to the sensitivities of the MENA region, firms have particular challenges, and auditors need to be aware of the following:

1. **Correspondent Banking Relationships**
   Auditors need to be aware of correspondent banking services provided, and that the respondent bank they are dealing with has adequate AML/CFT controls. Respondent banks whose controls are lax could exploit the vulnerabilities of a correspondent bank.

2. **Financial Exclusion and De-risking**
   According to a recently published article by Thomson Reuters, due to the high compliance cost, many banks have opted to take a broad-based “de-risking” approach rather than assessing business relationship risk on a case-by-case basis. This drives sectors and communities into financial exclusion, which erodes the financial system of the country. Most regulators have realized that this is a risky proposition due to financial exclusion issues and have voiced their dissent at blanket de-risking programs. Auditors need to ask the right questions and probe further if their firm has taken a decision of de-risking, and be aware of how this affects the firm internally and externally, particularly with regulators and other key stakeholders.

3. **Trade Relationships With Neighboring Countries, Particularly if They Are High Risk**
   Trade relationships with neighboring MENA countries are not only vital for the economy, but at times, unavoidable. Auditors must check to see if risks have been mitigated, and, if not, this must be highlighted.

4. **Cash-Intensive Businesses, Especially for MENA Countries**
   The general perception of cash being high risk is correct, but for MENA countries, this is a common method of conducting business, due to the economies being cash-rich. Although some MENA jurisdictions may have a cash-reporting threshold, it becomes difficult to monitor cash-based transactions due to the high prevalence of cash transactions. With this scenario, auditors must find a balanced and reasonable method of verifying and validating cash-based transactions.

5. **Transhipment Hubs**
   Auditors need to be aware of the risks associated with transhipment hubs, particularly if their firm is operating in that environment. The ultimate destination of goods is critical as sanctioned entities, and jurisdictions use transhipment hubs as a mode to obscure the trail of goods. As an example, if a consignment is destined ultimately for a sanctioned country, typically a transhipment hub would be used between the country

---

of origin and the sanctioned country or entity. Firms operating in transhipment hubs need to be careful not to assist in the sequence of operation, either with trade finance or any other service.

6. Sanctions Screening, Internal Blacklists, Domestic Lists

An auditor in a MENA firm must understand the applicability and enforceability of sanctions lists. Country/region-specific lists, such as OFAC, the UK, and the EU, may not be applicable to the firm if the firm’s business is limited to local operations. However, a particular challenge is when a firm engages in a correspondent banking relationship, say in the U.S., for which the OFAC lists become vital, and, by default, are to be applied. Breaches of these lists could be a possible case for the relationship to be ceased.

Global Firms

Firms headquartered in matured jurisdictions with global operations often have a branch office or representative office in the MENA region. While the branches or representative offices predominantly act as marketing offices, customers are often onboarded through booking centers or business acceptance units located either at the headquarters or in a different location from the marketing office.

Auditors need to be aware of the following:

1. The Auditable Standard

Which standard to audit against—the global standard or the regional one?

It is a possibility that a firm’s internal auditor inadvertently misses auditing the firm against the local country standard. In the event that the global standard is higher than the country standard, this is an amenable approach. However, if the country standard is higher than the global standard, this could open up potentially non-compliance issues and possible regulatory breaches. When a firm is located in several countries, a good starting point for the auditor is to review the gap analysis conducted between global vs. regional policies, should there be one. If a gap analysis has not been conducted, a recommendation to do so must be made on an immediate and urgent basis.

2. Regional Awareness

The other challenge for auditors is the lack of awareness of regional dynamics and trends. As an example, an auditor who is based in London may have less awareness of MENA regional issues ranging from basic ones (such as the manner in which business is conducted) and KYC sensitivities to complex issues (such as MENA specific trends and typologies). The greater challenge is to understand the dynamics of the MENA market and the associated typologies, including factors such as de-risking, informal financial systems, trading partners, channels of payments, and reliance on third parties, etc.

3. Sanctions Screening, Internal Blacklists, Domestic Lists

It is widely known that most global firms have an exhaustive database of various sanctions, and generally subscribe to a database that is updated frequently. The issue arises when a country issues domestic sanctions pursuant to UNSCR 1373. Since these are domestic lists, firms may miss entering the lists in the database, mostly due to a lack of clarity in the roles of the local and global compliance offices. An audit must
probe whether the firm has received any such domestic lists, and whether these are embedded in the overall sanctions regime particular to that branch or representative office. The auditor must check whether reasonable controls are in place to ensure that the firm does not engage with the domestically sanctioned individuals and entities.

4. Transaction Monitoring Thresholds
Auditors also need to review the parameters and thresholds of the transaction monitoring system, which must align with the local business of the firm. As an example, other jurisdictions may have lower thresholds for cash deposits, whereas the MENA firms might consider higher thresholds subject to being complaint with legislation. Firms in the MENA region should calibrate their thresholds to adjust to the business needs, or there could be an unjustified number of red flags generated. The risk in this approach is that genuine red flags may get “lost” between thousands of other red flags and not be actioned or investigated in time.

5. Auditors Working Remotely
The other challenge is when an auditor is asked to perform his or her work remotely. The major consideration here is on “effectiveness,” as working remotely precludes the important element of physically verifying data and the “gut feeling” that is a natural instinct of an auditor.

However, this is sometimes unavoidable, as firms have a centralized audit team that is assigned different countries on a rotation basis, and depending on resource availability, is asked to audit by remote means. A possible solution to this could be either to dedicate a sub team to a country or to have a MENA region team. There are pros and cons for each choice, and firms must choose the most effective.

Auditing ML/TF Risks: Where and What to Look For

The below highlights pointers, good and bad practices of risk assessments, that may be of assistance while undertaking the audit of risk assessments.

- **Regulatory Obligation**
  The first consideration is for auditors to check whether conducting a risk assessment is a rule requirement. If it is indeed a requirement, and this is not met appropriately, then firms could face AML/CFT rule breaches, possible fines, sanctions, or public censures.

- **Guidance Issued by Regulators**
  When a regulator issues guidance on auditing an ML/TF risk assessment, it is recommended that the guidance be considered and incorporated into the audit scope and methodology.

- **Relevant Business Units**
  The assessment is incomplete if it does not include all of the relevant business units and is not appropriate for the firm’s size, nature, and complexity.
• **Factors**  
Auditors need to check the rule requirement, as some jurisdictions are prescriptive, to include the risk factors within the rules.

• **Customer Risk**  
The risk assessment is incomplete if the customer risk is not addressed sufficiently. As an example, a customer may be a salaried individual as well as have additional sources of income. While most firms factor in the customer’s “salary” status (in most cases as low risk), the failure to account for his or her other income may not reflect the correct risk rating.

• **Product/Service Risk**  
The ML/TF risks associated with the products and services must be addressed. A simple example is that firms are able to include an exhaustive list of the product and service specifications in the risk assessment, but fail to identify the risks associated with the product and service.

• **Interface Risk**  
Some firms fail to address the interface risk in entirety, and some firms integrate interface risk into customer risk. While this is not an issue, this must be clearly stated and undertaken in a comprehensive manner. Not identifying interface risk entirely is critical for the risk assessment. Further, if it is a rule requirement, then not identifying the interface risk is a breach of the rules.

• **Jurisdiction Risk**  
Firms are expected to risk-rate countries. A pragmatic approach is to rely on well-known, vendor-supplied lists. Smaller firms may not have the financial resources to subscribe to external vendors and therefore create internally a “country risk list” from externally available reliable sources. While both ways are acceptable, the issue arises when the country list is static and has not been updated. For example, a firm’s current risk assessment incorporates a list of country risk ratings from 2014. The lists were not updated and contained countries that had currently higher risk ratings, or alternatively, jurisdictions that had lower risk ratings.

• **Mitigating Controls**  
At times, firms do not adequately assess the mitigating factors, and this is often a more generalized approach limited to a few paragraphs. Auditors need to check if the controls are mapped to the risks.

• **Scoring and Weighting Mechanism**  
Scoring with appropriate weights puts into perspective the critical areas of focus, with more weights being assigned to higher risk areas. Auditors need to check if the scoring mechanism is fit for the purpose.

• **Residual Risk Rating**  
Poor practices range from not conclusively arriving at the firm’s risk rating—i.e., low, medium, or high—or alternatively stating the risk rating, which in most cases are low with no justifiable basis.
Key Takeaways and Conclusion

The top three takeaways are:

- A risk assessment is not optional. Even if your regulator does not make it a mandatory requirement, nevertheless, a risk assessment must be conducted, as it is fundamental in identifying the ML/TF risks, threats, vulnerabilities, and consequences.

- Inadequately identifying the ML/TF risks or unjustifiably lowering the risk rating of the firm only exposes the entity to a higher degree of risk. At the conclusion of a risk assessment, most MLROs/ risk owners are content to say that their firm is a “low risk.” While this is not a problem if the risk is truly low, creating a false perception of a lowered risk is dangerous and exposes the firm to unknown threats and vulnerabilities.

- The selection criteria of auditable items is paramount. It is acknowledged that it is necessary for auditors to cover, in a broad manner, all aspects of ML/TF risks. However, it is critical that a drill down be conducted on higher risk issues, which makes the audit more meaningful and beneficial. Audit stakeholders, such as the firm’s senior management and regulators, are keen on knowing the threats, vulnerabilities, and control gaps as opposed to simply being told that “the audit was satisfactory.”

A risk assessment is a thought-out documented process to identify ML/TF risks. Money laundering and terrorist financing targets a firm’s weakest link, and that is why a firm’s control environment is only as good as its weakest link. A gap in its control environment opens up a plethora of threats, which would create a domino effect to the entire firm.

The need of the hour is for an audit to extend beyond just ensuring a firm has an ML/TF risk assessment, but also to validate the risk assessment and assess whether the risk assessment is fit for purpose.
# Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering/Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>DFSA</td>
<td>Dubai Financial Services Authority</td>
</tr>
<tr>
<td>DNFBP</td>
<td>Designated Non-Financial Business or Profession</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>Firm</td>
<td>Financial Institution and Designated Non-Financial Business or Profession</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>MLRO</td>
<td>Money Laundering Reporting Officer</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control (Treasury Department)</td>
</tr>
<tr>
<td>QFCRA</td>
<td>Qatar Financial Centre Regulatory Authority</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorist Financing</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNSCR</td>
<td>United Nations Security Council Resolutions</td>
</tr>
<tr>
<td>U.S.</td>
<td>United States of America</td>
</tr>
</tbody>
</table>
References


Countries assessment guideline. Reserve Bank of New Zealand. 


European Union Sanctions. 
https://www.sanctionsmap.eu/#/main?search=%7B%22value%22:%22%22,%22searchType%22:%7B%22id%22:1,%22title%22:%22regimes,%20persons,%20entities%22%7D%7D.


The Financial Secrecy Index. Tax Justice Network. 


## Appendix A – An Audit Checklist for Risk Assessments

### Pre-Audit

<table>
<thead>
<tr>
<th>Description</th>
<th>Items to be Considered</th>
<th>Check ✓ / X / NA</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Meetings with senior management/business line heads | • Meetings to discuss the current business strategy, changes in the firm affecting the business, previous audit findings, and upcoming audit focus  
• Meetings with individual business heads to understand changes, operational issues, self-reported challenges, etc.                                                                                         |                  |       |
| Meet with regulators prior to the audit          | • Meet with regulators to inform them of the audit  
• Incorporate any issues highlighted by regulators  
• Typologies/trends analysis issued by regulators  
• Factor in any regulatory guidance issued, and seek clarifications if required                                                                                                                                  |                  |       |
| Determine the scope of the audit                 | • Is it a full-scope or targeted audit?  
• Validation of previous audit issues/open matters  
• Incorporate regulatory guidance on audits, if issued                                                                                                                                                         |                  |       |
| Representative sampling                          | • A representative sampling percentage (for customer files, transactions, red flags, etc.) must be agreed upon prior to the audit commencing  
• Appropriate sign-offs are required                                                                                                                                                                             |                  |       |
| Selection of auditees                            | • Document the criteria for auditee selection  
• Interview notes to be retained                                                                                                                                                                                      |                  |       |
| Selection of auditors                            | • Appropriate skills, knowledge, and experience  
• Consider if they were involved in any previous audits                                                                                                                                                           |                  |       |
<table>
<thead>
<tr>
<th>Description</th>
<th>Items to be Checked</th>
<th>Check ✓/✗/NA</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Consider these focus areas | **General Areas**  
  - The ownership and corporate structure—taking into account whether the firm is international, foreign, or domestic, a parent company, subsidiary, branch, or any other kind of establishment  
  - The level of complexity and transparency in the firm  
  - The current customer base, onboarding customers for a new segment, and diversification into emerging markets  
  - The nature and complexity of the products and services provided and the activities and transactions carried out  
  - The delivery channels used, including the free provisions of services and the use of agents or intermediaries and non-face-to-face mechanisms  
  - The geographical area of the business activities, in particular where they are carried out in high-risk countries, as well as, if applicable, the countries of origin or establishment of a significant part of the firm’s customers  
  - The quality of internal governance arrangements in place and the prevailing “compliance culture”  
  - Written AML/CFT policies, procedures, systems, and controls—whether it remains fit for purpose  
  - The control environment | | |
| | **Specific Areas**  
  - High risk customers  
  - Sudden surge in activity for newly opened accounts or accounts opened for a niche service  
  - Have any new products and services been introduced since the last audit, or have any changes been made to the existing products and services? If yes, has an ML/TF product risk assessment been carried out?  
  - Transactional activity with high risk countries | | |
- Red flags and methods of resolution
- STRs: internal and external, paying attention to those internal STRs that were not reported externally, and the method of resolution
- Adequacy of the identification of ML/TF risks
- Residual risk rating of the firm
- Risk appetite of the firm
- Senior management’s awareness of the residual risk rating and acceptance of the risk
- Appropriateness of the frequency of conducting risk assessments
- Methodology of risk assessments (the threat assessment methodology)

### Working notes
- All notes to be sequenced and documented
- Regulators may request the working notes in support of the grading of the audit

### Sample of customer files
- A representative sample of high-, medium-, and low-risk customers, while focusing more on the high risk customers
- Representative sample of new customers
- Representative sample of who closed accounts or discontinued services in less than a year of opening the accounts

### Communication of preliminary findings
- Preliminary findings to be communicated to the auditees—as a cautionary measure to identify any factually incorrect findings
- Discuss remediation timelines

### Post-Audit

<table>
<thead>
<tr>
<th>Description</th>
<th>Items to be checked</th>
<th>Check ✓ / X / NA</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closure meetings with the business heads and Audit team</td>
<td>The draft report is to be presented and mutually acceptable remediation dates to be agreed upon</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit report</td>
<td>• The final report is to be communicated to all concerned</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Senior management sign-off is necessary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tracking mechanism</td>
<td>• An interim check-in before the final remediation date is recommended to ensure that the remediation is on track</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the remediation is not on track, then matters must be escalated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Closure</td>
<td>• Upon remediation, matters must be closed and communicated to all concerned</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Any outstanding matters that require an extension must receive appropriate sign-offs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>