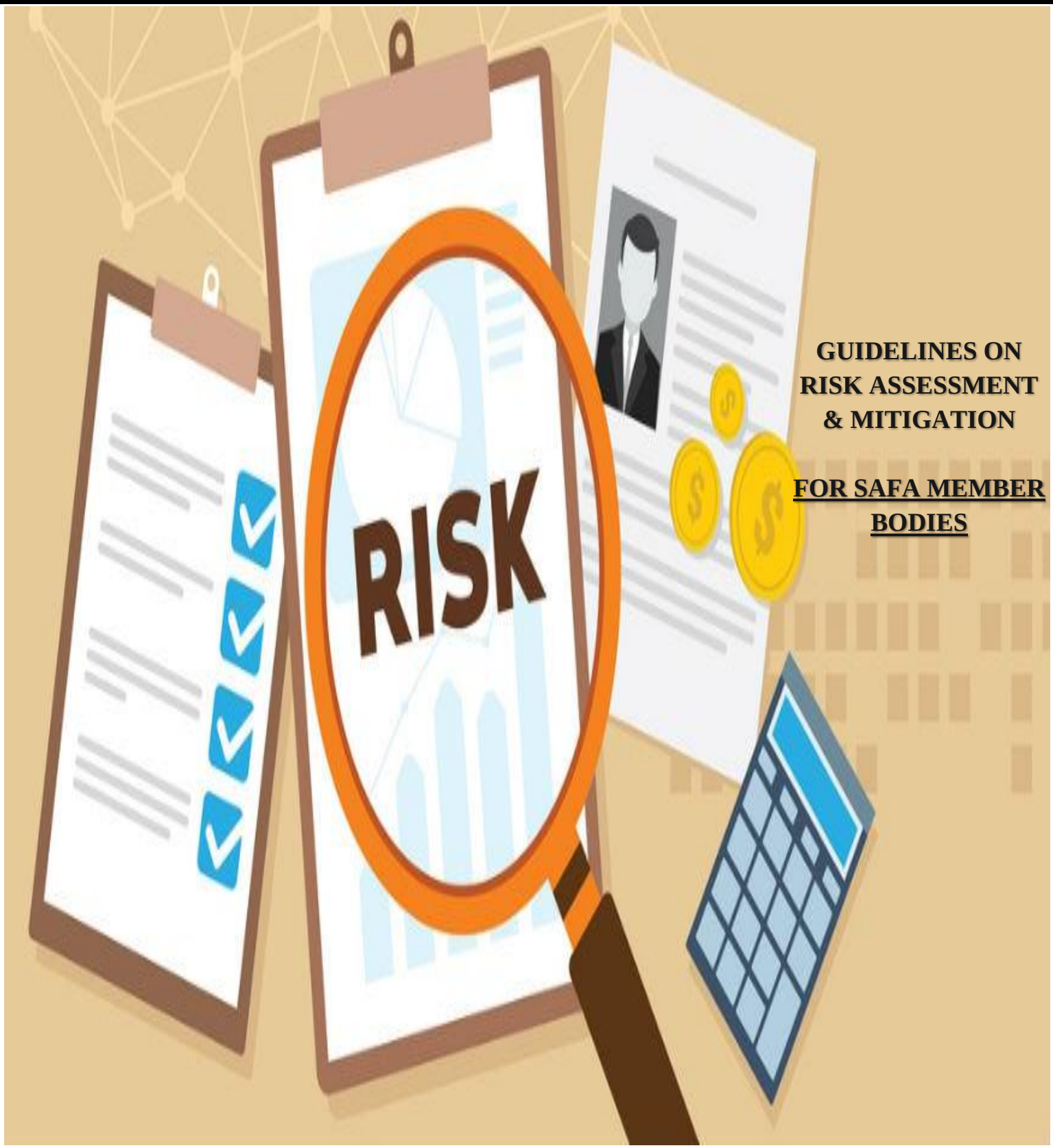
GUIDELINES ON RISK ASSESSMENT & RISK MITIGATION



INTRODUCTION

In the realm of financial security and integrity, the assessment and mitigation of risks associated with money laundering and terrorist financing are paramount. This critical process involves a comprehensive examination of potential threats, their likelihood, and the potential consequences they pose to the financial system.

A fundamental approach to this challenge is the adoption of a risk-based methodology. By employing such an approach, entities can tailor their measures according to the specific risks they face, ensuring that resources are allocated efficiently and effectively.

At the core of this methodology lies the understanding that not all risks are equal. Some risks may pose a significant threat to financial stability and security, while others may be more manageable. Therefore, a nuanced approach is necessary to identify, assess, and address these risks appropriately.

Guided by international standards and best practices, organizations and regulatory bodies develop frameworks to conduct risk assessments and implement corresponding mitigation strategies. These frameworks serve as crucial tools in combating financial crime and safeguarding the integrity of the financial system.

LEGAL OBLIGATION

1. The South Asian countries are under legal obligation to implement the FATF Recommendations on Risk Assessment, on account of being a responsible member of the United Nations.
2. To fulfill these obligations, these countries depend on various legal provisions outlined within their respective Laws and Regulations pertaining to Anti-Money Laundering (AML). It's important to note that these legal provisions can vary from one country or organization to another, reflecting the unique regulatory frameworks and priorities of each jurisdiction.

COUNTRY WIDE RISK ASSESSMENT

Countries should undertake comprehensive steps to identify and evaluate money laundering and terrorist financing risks within their jurisdiction continuously. The purpose of this assessment is multifaceted:

(i) to inform potential adjustments to the country's AML/CFT regime, including legislative and regulatory changes;

(ii) to aid in the allocation and prioritization of resources dedicated to AML/CFT efforts by competent authorities; and

(iii) to provide information for AML/CFT risk assessments conducted by reporting entities.

It is imperative for countries to maintain up-to-date assessments and establish mechanisms for disseminating assessment results to all relevant competent authorities.

ENTERPRISE RISK ASSESSMENT

The purpose of the enterprise risk assessment for a reporting entity is to identify which customers, geographic regions, services and channel of delivery that are higher or lower risk for ML / TF, and to focus more attention on the higher risk areas. In other words, a risk based approach (RBA).

The key purpose of an ML / TF enterprise wide risk assessment is to drive improvements in risk management through identifying the general and specific ML and TF risks a reporting entity is facing, determining how these risks are mitigated by the reporting entity's AML / CFT programme controls, and establishing the residual risk that remains for the reporting entity. The reporting entity's AML / CFT programme must be based on the reporting entity's risk assessment.

The risk assessment should also include proposed mitigation measures needed, including AML / CFT controls and procedures identified by the risk assessment.

It is pertinent to highlight that the ML / TF enterprise risk assessment is not a one-time exercise and must be kept up to date. Based on the international practices, it should be reviewed and updated at least once every two years, or when there are material or significant changes in specified services provided by the reporting entity.

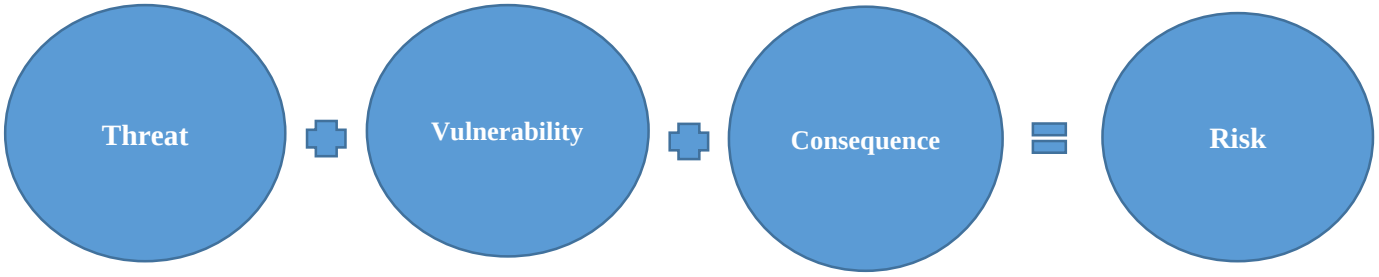
HOW TO CONDUCT AN ENTERPRISE RISK ASSESSSMENT?

When conducting an enterprise risk assessment, the reporting entity shall comply with its obligations under the AML / CFT legislations and choose the method of risk assessment that best suits it.

The following explains the key steps in conducting an enterprise wide risk assessment i.e. understand the meaning of ML / TF risk, identify the risk categories and then assess the risk, including quantitative and qualitative information collection.

Step # 1: What is ML/TF Risk:

It is commonly accepted that risk is a function of three factors - threat, vulnerability and consequence; as shown below:



Threat: A threat is a person or group of people with the potential to cause harm by ML or TF.

Vulnerability: A vulnerability comprises those things that can be exploited by the threat or that may support or facilitate its activities.

Consequence: A consequence refers to the impact or harm that a threat may cause if eventuated. When determining impact of ML / TF, the reporting entity may consider a number of factors, including:

a. Nature and size of your business (domestic and international);
b. Potential criminal, financial and reputational consequences;
c. Terrorism-related impacts;
d. Wider criminal activity and social harm;
e. Political impact;
f. Negative media.

Step # 2: Identify the Risks:

Generally, AML/CFT Legislations specify the following four mandatory risk categories:

a. Customer risk
b. Countries or geographic risk (internal and overseas)
c. Products services risk (including technology)
d. Transaction or delivery channel risk (including technology)

Weighting: The above risk categories may be weighted, or the reporting entity may decide to assign equal weighting to each e.g. 25%. It depends on the nature of the business. For example, if the reporting entity has no international exposure then geographic risk may not be a significant risk category for its risk assessment. The converse may be true if the reporting entity has significant international exposure.

Other risk categories: When conducting the reporting entity's ML / TF enterprise risk assessment, the risk categories need not be limited to the above categories, but the risk assessment must cover the above four risk categories. The risk assessment could include other qualitative risk categories, such as the institutions the reporting entity deals with e.g. lawyers, real estate agents, money remitters etc.

Business lines: The enterprise risk assessment should identify the risk categories in the context of nature of the reporting entity's business activities i.e. which business lines (e.g. that generate revenue through professional fees) deliver the specified services subject to AML / CFT, and/or have greater exposure to customer, geographic, products and services, and their delivery channel risks?

The reporting entity may identify and assess the risk by using risk indicators under each of the risk categories. Following are the major risk indicators which are generally used globally including in FATF guidance documents:

➢ Customer Risk:

- This risk category is considered as a threat to the entity's business. The following question should be considered, "Does the customer or its beneficial owners have characteristics known to be frequently used by money launderers or terrorist financiers?"
- Customer risk may be summarized as follows:
  - Type of customer: For example, an individual who has been entrusted with a prominent public function (or immediate family member or close associate of such an individual) may present a higher risk e.g. politically exposed persons (PEPs), inactive company, links to offshore tax havens and personal asset holding arrangements;
  - Transparency of customer: For example, persons that are subject to public disclosure rules, e.g. on exchanges or regulated markets (or majority-owned and consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, may indicate lower risk.
  - Customers where the structure or nature of the entity or relationship makes it difficult to identify the true beneficial owners and controllers may indicate higher risk e.g. those with nominee directors or nominee shareholders or which have issued bearer shares;
  - Type and complexity of ownership: For example, the use of overly complex or opaque structures with different layers of entities situated in two or more countries and cross border transactions involving counterparts in different parts of the world, the unexplained use of corporate structures and express trusts by customers, and the use of nominee and bearer shares may indicate higher risk;
  - In the case of an express trust, the nature of the relationship between the settlor(s) and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power. For example, a trust that has company or another trust as a beneficiary may indicate higher risk. While a trust that is established for the benefit of the close family of the settlor may indicate a lower risk;
  - Sector risk: Reporting entities should consider the sectors in which their customer has significant operations, and take this into account when determining a customer's risk profile. When considering what constitutes a high risk sector, entities should take into account the findings of the most recent National Risk Assessment. For example, a customer engaged in higher risk trading activities or engaged in a business which involves significant amounts of cash may indicate higher risk;
  - Reputation of customer: For example, a well-known, reputable person, with a long history in its industry, and with abundant independent and reliable information about it and its beneficial owners and controllers may indicate lower risk;
  - Behavior of customer: For example, where there is no commercial rationale for the service that is sought, or where undue levels of secrecy are requested by a customer, or where a customer is reluctant or unwilling to provide adequate explanations or documents, or where it appears that an "audit trail" has been deliberately broken or unnecessarily layered, this may indicate higher risk;

- The regularity or duration of the relationship: For example, longstanding relationships involving frequent customer contact that result in a high level of understanding of the customer relationship may indicate lower risk;
- Delegation of authority by the applicant or customer: For example, the use of powers of attorney, mixed boards and representative offices may indicate higher risk;

➢ Geographic Risk:

- This risk category may be considered both a threat and vulnerability. A reporting entity should consider the following question "Are our customers established in countries or regions that are known to be used by money launderers or terrorist financiers?" Though it should be borne in mind that lower risk and legitimate commercial enterprises may be located in high risk countries.

- Other major factors include the following:
  - ineffective AML / CFT measures
  - ineffective rule of law and economic stability
  - high levels of organized crime
  - prevalence of bribery and corruption
  - association with terrorism and TF

- Information on the above should be based on credible sources. The "credible sources' refer to information that is produced by well-known bodies, are generally regarded as reputable, and that make such information publicly and widely available. These include:
  - FATF: http://www.fatf-High risk and other monitored jurisdictions
  - FATF-style regional bodies e.g. APG

➢ Product and Services Risk (including technology risk):

- The products and services a reporting entity offers are vulnerabilities that your customers, associates or counterparties may attempt to exploit to conduct ML or TF. A reporting entity should consider the following question "Do any of our services have attributes known to be used by money launderers or terrorist financiers?" The specified services have already been identified already as higher risk, and therefore subject to the AML / CFT legislations.

- Within those specified services, there are other factors that will further increase the risk. Some of the main ones are as follows:
  - Does your reporting entity accept large cash payments or virtual currency?
  - Does the product/service allow for anonymity (i.e. you do not physically see or meet the actual

- customer)?
- Does the product/service disguise or conceal the beneficial owner of your customer?
- Does the product/service disguise or conceal the source of wealth or funds of your customer?
- Does the product/service allow payments to, or from third parties?
- Does the product/service commonly involve receipt or payment in cash?
- Does the product/service allow for the movement of funds across borders?
- Does it hold boxes, parcels or sealed envelopes in safe custody for customers?
- Does it place funds in customer, nominee or other accounts, where funds are mingled with others' funds?

➢ Delivery Channel Risk:

- How your entity delivers products and services are vulnerabilities that your customers, associates or counterparties may attempt to exploit to conduct ML or TF. The entity should consider the following question, "Does the fact that I am dealing with the customer non face to face pose a greater ML / TF risk?" The higher risk factors could include the following:
  - Indirect relationship with the customer – dealing through intermediaries or other third parties; and
  - Does your business have non-face-to-face customers (via post, telephone, internet or via intermediaries)?
  - Do you provide your products/services to overseas jurisdictions?

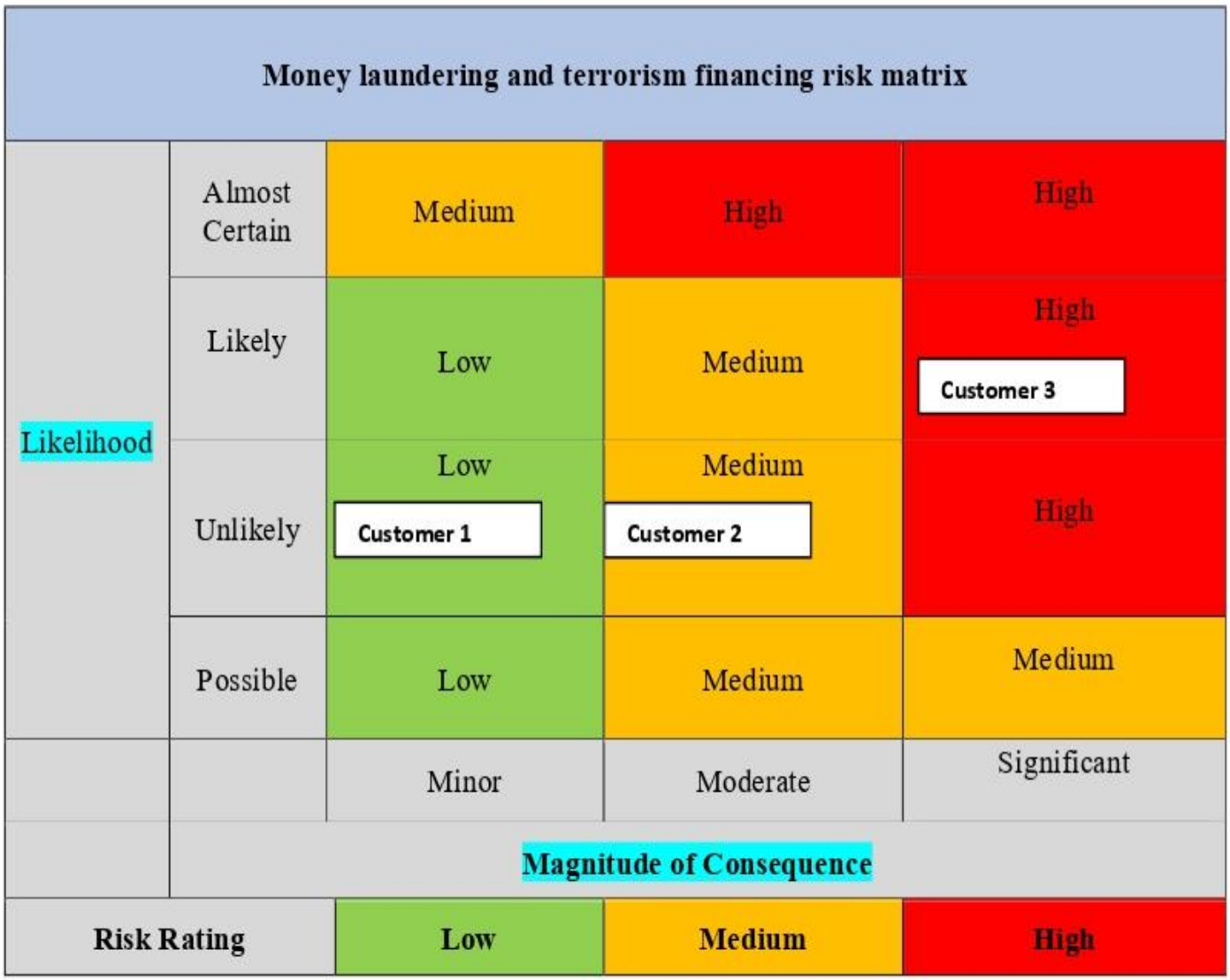
Step # 3: Assess the Risk:

Likelihood: In order to assess the risk based on the equation i.e. Threat + Vulnerability + Consequence = Risk, there is an additional element that needs to be assessed, which is the likelihood of the event i.e. ML or TF. Likelihood could be (i) Almost certain (ii) Likely (iii) Unlikely and (iv) Possible.

The following are definitions for the different categories of likelihood:

- Almost certain: There is a high probability of ML / TF occurring in this area of the business
- Likely: There is a medium probability of ML / TF occurring in this area of the business
- Unlikely: There is a low probability of ML / TF occurring in this area of the business
- Possible: There is a minuscule probability of ML / TF occurring in this area of the business.

When assessing the ML / TF risk, the following matrix, which is commonly refer to as a "heat map", with Likelihood and Consequence scenarios provides a more structured approach.



QUANTITATIVE AND QUALITATIVE INFORMATION FOR ENTERPRISE RISK ASSESSMENT:

Information needed for an enterprise risk assessment may be collected from various sources, as summarized below:

a. **Internal Information:** The reporting entity's own information about the practice – how many business lines, locations, main services, how many accountants providing specified services, customers groups, technologies used etc.

   Information from within the reporting entity may be collected via a questionnaire or a telephone meeting, or face to face meeting. Depending on how customer records are kept, it may take some time to extract information needed. It is unlikely to obtain all the required information, but should be sufficient for informed conclusions to be made.

b. **National Risk Assessment:** The reporting entity should take account of the findings of the latest National Risk Assessment at country level to inform its enterprise risk assessment of the ML and

TF threat environment, and including high risk activities and sectors.

c. **International:**
   - FATF (FATF: http://www.fatf-High risk and other monitored jurisdictions) and FATF-style regional bodies
   - Supra-national or international bodies such as the United Nations Security Council (https://scsanctions.un.org/search/), International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

RISK MANAGEMENT:

Countries and reporting entities should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities.

CLIENT RISK ASSESSMENT:

The enterprise risk assessment is separate to a customer risk assessment; the latter must be completed before a new customer is accepted, and the risk rating reviewed and updated, if necessary, under ongoing Customer Due Diligence (CDD).

The enterprise risk assessment and customer risk assessments are closely linked, but they are not exactly the same. A reporting firm is required to both (a) conduct the enterprise risk assessment and (b) assess individual customer risk, particularly for new customers. The enterprise risk assessment provides a macro assessment of risk in your firm, while the individual customer risk assessment is a micro perspective.

Customer risk assessment determines the risk profile of the customer only. That said, once you have completed your enterprise risk assessment, the conclusions on the risk variables (i.e. customer, geography, products and services, and delivery channel) will inform your customer risk assessments.

As part of the customer risk assessment process, it is essential to adhere to Know Your Customer (KYC) guidelines, as detailed in the approved document “Guidance document on CDD” circulated the previous year by the SAFA AML Committee. This ensures that comprehensive due diligence is conducted on each customer, allowing for the identification and verification of their identity, beneficial ownership, and other pertinent information relevant to mitigating the risk of money laundering and terrorist financing. Enhanced due diligence measures should be applied in situations where the risk of money laundering or terrorist financing is higher. This includes gathering additional information about the customer, conducting more thorough verification of identity, and obtaining information about the source of funds and the purpose of

transactions.

The risk assessment methodology for the customer risk assessment is the same as the enterprise risk assessment:

The customer risk assessment must be sufficiently precise to allow the development of a risk matrix that grades customers, products, geography, and delivery channels into risk categories to derive an overall customer risk rating. Each customer must receive an initial AML / CFT risk rating at the beginning of the business relationship, and it must be kept current based on updates and changes in the relationship. For example, if a customer is inactive over a longer period of time, the risk rating may need to be revised.

Lower risk: For specified services subject to AML / CFT legislations, this would be not common for reporting firms, except a few instances. For example, if the customer is a publicly listed company.

Medium risk: Standard customer due diligence is the most common level of due diligence and would be the most common situation facing the reporting firm.

Higher risk: When a customer or beneficial owner of a customer is a (i) politically exposed person (PEP), and (ii) the business relationship and transactions are with natural and legal persons from countries for which this is called for by the FATF, they are automatically higher risk and subject to enhanced due diligence.

BEST PRACTICES IN RISK ASSESSMENT:

Some globally recognized best practices related to risk assessment include:

Utilization of Risk Assessment Frameworks: Adopting internationally recognized risk assessment frameworks provides a structured approach to risk identification and mitigation. Further, consider adopting an integrated risk management framework that combines AML/CFT efforts with other risk management areas such as cybersecurity, operational risk, and compliance. This ensures a comprehensive approach to risk mitigation. Implement a unified risk dashboard that provides a real-time overview of all risk factors, enabling better decision-making and resource allocation.

Integration of Emerging Risks: Continuously monitoring and incorporating emerging risks, such as those related to technological advancements, geopolitical developments, or changes in regulatory requirements,

ensures that risk assessments remain relevant and proactive.

Scenario & Behavioral Analysis: Conducting scenario-based risk assessments helps organizations anticipate and prepare for various potential threats and their potential impacts. This approach allows for the testing of resilience strategies and the identification of vulnerabilities under different hypothetical scenarios. Further, consider implementing behavioral analytics to develop detailed profiles of customer behavior. This helps in identifying deviations from normal behavior that may indicate fraudulent activities. Use psychometric analysis to understand the psychological traits and behaviors of individuals, providing deeper insights into potential risks.

Cross-Border Collaboration: Engaging in cross-border collaboration with other financial institutions, regulatory authorities, and law enforcement agencies facilitates the sharing of intelligence and best practices, enabling a more comprehensive assessment of global risks and threats.

Dynamic Risk Rating Systems: Implementing dynamic risk rating systems enables organizations to adjust risk ratings for customers, products, and geographic locations in real-time based on changing risk factors and emerging trends. This flexibility ensures that risk assessments remain accurate and up-to-date.

Continuous Monitoring: Implementing robust systems for continuous monitoring of transactions, customer behavior, and external risk factors allows organizations to detect suspicious activities promptly and take appropriate risk mitigation measures.

Expert Consultation: Seeking input from subject matter experts, such legal advisors, and industry specialists, enhances the depth and accuracy of risk assessments, especially in complex or high-risk scenarios.

Documentation and Audit Trails: Maintaining detailed documentation and audit trails of risk assessment processes, including assumptions, methodologies, and decision-making criteria, ensures transparency and accountability, facilitating regulatory compliance and internal reviews.

Regular Training and Awareness Programs: Providing regular training and awareness programs to employees on risk assessment methodologies, red flags, and compliance requirements ensures that staff are equipped to identify, assess, and respond to risks effectively. Develop gamified training modules for employees to make learning about AML/CFT regulations more engaging and effective. These modules can simulate real-world scenarios and test employees' decision-making skills. Offer certification programs that reward employees for completing advanced AML/CFT training courses, ensuring continuous professional development.

Independent Review Mechanisms: Establishing independent review mechanisms, such as internal audit or compliance committees, ensures impartial oversight of risk assessment processes, identifies gaps or weaknesses, and facilitates continuous improvement.

Incorporation of Artificial Intelligence (AI) and Machine Learning (ML): Implementing AI and ML technologies to enhance the detection and prediction of suspicious activities. These technologies can analyze large datasets to identify patterns and anomalies indicative of money laundering and terrorist

financing. Use AI/ML algorithms to automate risk scoring of transactions and customers, allowing for real-time updates and more accurate risk assessments.

Data Privacy and Protection Measures: Ensure robust data privacy and protection measures are in place to safeguard sensitive customer information. This includes encryption, access controls, and regular security audits. Align data management practices with the Data Protection laws to ensure compliance and build customer trust.

By implementing these specific best practices, organizations can enhance the effectiveness and reliability of their risk assessment processes, thereby mitigating financial crime risks and safeguarding the integrity of the financial system.

GLOSSARY	
CDD	Customer/Client Due Diligence
AML	Anti-Money Laundering
ML	Money Laundering
CFT	Counter-Terrorism Financing
TF	Terrorist Financing
FATF	Financial Action Task Force
RBA	Risk Based Approach
PEPs	Politically Exposed Persons

MULTIPLE CHOICE QUESTIONS (MCQs)

1) What is the primary purpose of adopting a risk-based methodology in combating money laundering and terrorist financing?
a) To allocate equal resources to all potential risks
b) To tailor measures according to specific risks faced
c) To eliminate all risks completely
d) To prioritize risks based on regulatory requirements

2) Which of the following is NOT a mandatory risk category specified in AML/CFT legislations?
a) Customer risk
b) Geographic risk
c) Product and services risk
d) Internal audit risk

3) How often should an ML/TF enterprise risk assessment be reviewed and updated based on international practices?
a) Once every year
b) Once every three years
c) Once every two years
d) Once every five years

4) Which of the following is NOT considered as a risk category in the enterprise risk assessment?
a) Transaction or delivery channel risk
b) Supplier risk
c) Customer risk
d) Product and services risk

5) What does the Likelihood component in the risk assessment matrix refer to?
a) The consequence of ML/TF occurring
b) The probability of ML/TF occurring
c) The potential vulnerabilities exploited by ML/TF
d) The impact of ML/TF on the financial system

6) What is the primary purpose of conducting a customer risk assessment?
a) To identify weaknesses in the AML/CFT program
b) To allocate resources for compliance purposes
c) To determine the risk profile of individual customers
d) To assess the overall risk of the financial system

7) Which of the following is generally NOT a best practice related to risk assessment?
a) Integration of emerging risks
b) Continuous monitoring
c) Static risk rating systems
d) Scenario analysis

8) What does the term "CDD" stand for in the context of AML/CFT?
a) Customer Decision Database
b) Counter Due Diligence

c) Customer/Client Due Diligence
d) Compliance and Documentation Division

Correct Answers:

b) To tailor measures according to specific risks faced
d) Internal audit risk
c) Once every two years
b) Supplier risk
b) The probability of ML/TF occurring
c) To determine the risk profile of individual customers
c) Static risk rating systems
c) Customer/Client Due Diligence