MONEY LAUNDERING / TERRORIST FINANCING /PROLIFERATION FINANCING

RISKS ASSESSMENT GUIDELINES

FOR

SUPERVISED FINANCIAL INSTITUTIONS (SFIs)

DECEMBER 2022

Glossary of acronyms

AMLA	Ant-Money Laundering Act
AML	Ant-Money Laundering
AML/CFT/CPF	Anti-Money Laundering/Countering the Financing of Terrorism and Proliferation Financing
BCBS	Basel Committee on Banking Supervision
BOU	Bank of Uganda
CDD	Customer Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force.
FIA	Financial Intelligence Authority
FSAPs	Financial Sector Assessment Program
ML	Money Laundering
MLCO	Money Laundering Control Officer
PEPs	Politically Exposed Persons
PF	Proliferation Financing
SFIs	Supervised Financial Institutions
TF	Terrorism Financing
VASPs	Virtual Asset Service Providers

1. Background and Legal Requirements for conducting ML/TF/PF Risk Assessment

1.1 The Financial Action Task Force (FATF) recommendations set standards for jurisdictions to apply a **Risk-Based Approach (RBA)** to implementing anti-money-laundering and combating the financing of terrorism and proliferation financing[1] (AML/CFT/CPF) measures.

1.2 Applying AML/CFT/CPF Risk Based Approach means that, the Country, Bank of Uganda (BOU) and the Supervised Financial Institutions (SFIs) should each identify, assess and understand the ML/TF/PF risks to which they are exposed to and entails risk mitigation measures commensurate with the identified risks in order to manage and mitigate them effectively. This process is referred to as **"Risk Assessment".**

1.3 At the National/Country level, Uganda identifies, assesses, and understands the money-laundering (ML), terrorism financing (TF), and proliferation financing (PF) risks, by conducting the **National Risk Assessment,** while at the Sectoral Level, BOU conducts the Risk Assessment for the Banking, Foreign Exchange Bureaus & Money Remitters Sectors.

1.4 Therefore, at the entity level and in accordance with the requirement stipulated in Section 6A (a) of the Anti-Money Laundering Act (AMLA) (as amended) 2022 and Regulation 8 (1) of the AML Regulations 2015, SFIs are required to take appropriate steps to identify, assess and monitor their ML/TF/PF risks. Hence, SFIs should conduct the entity level ML/TF/PF Risk Assessment, establish risk mitigations that should be undertaken including policies, procedures, and controls and assess the adverse consequences of non- compliance with the applicable AML/CFT/CPF laws and regulations.

1.5 In addition to the entity level ML/TF/PF Risk Assessments, SFIs should also identify, assess and, take appropriate measures to manage and mitigate the ML/TF/PF risks that may arise in relation to the development of new products and new business practices; including new delivery mechanisms for products and services; and the use of new or developing technologies for both new and pre-existing products. This requirement is stipulated in Section 6A (2) of the AMLA (as amended) 2022.

1.6 The Risk Assessments mentioned in part 1.5. should be conducted **prior** to the launch of the new products or business practices or a new technology for both new and pre-existing products or services and the use of new or developing technologies for both new and pre-existing products. This

[1] In the context, ***"proliferation financing risk"*** refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations *(refer to the TFS Guidelines 2022)*

requirement is stipulated in Section 6A (3) of the AMLA (as amended) 2017 and Regulations 9 of the AML Regulations 2015.

1.7 Therefore, pursuant to Section 6 (27) of the AMLA (as amended) 2017 BOU has prepared these Guidelines to assist SFIs to implement and comply with the AML/CFT/CPF requirements regarding conducting the Risk Assessment.

1.8 Since the nature of the TF differs from that of ML, the risk assessment must cover an analysis of TF risk. Since the funds used for TF may originate from legal sources, the nature of the sources may vary depending on the given factors, however, when the source of TF originates from criminal activities, the risk assessment related to ML is also applicable to TF.

1.9 The TF counter measures which the SFIs may have in place shall overlap with the AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, and escalation of suspicions and liaison relationships with the authorities. The guidance provided in these guidelines, therefore, applies to CFT as it does to AML, even where this is not explicitly mentioned.

2. International Standards for ML/TF/PF Risk Assessment

2.1 The key AML/CFT/CPF technical requirement for SFIs to conduct Risk Assessment is contained in Recommendation 1 and its accompanying Interpretive notes.

2.2 Additionally, the Basel Core Principles of Effective Banking Supervision also require SFIs to have in place sound risk management programs to address all kinds of risk including ML/TF/PF risks by putting in place adequate mitigation measures such as policies and processes, to prevent the SFI from being used for criminal activities. The sound risks management program should be risk based and informed by the SFI's own assessment of its ML/TF/PF risks.

3. Objectives of the ML/TF/PF Guidelines

3.1 The objective of these Guidelines is to assist SFIs to have quality and effective ML/TF/PF risks assessment and ML/TF/PF risk management systems that are appropriate and proportionate to the risks they are exposed to. SFIs are required to develop AML/CFT/CPF control measures that are commensurate to the risk identified and prevent the ML/TF/PF. Therefore, the Objectives of these guidelines are to:

a) Provide a standard and common understanding of ML/TF/PF Risk Assessment amongst the SFIs in the Banking Sector.

b) Outline the minimum recommended steps for conducting the ML/TF/PF risk assessment by the SFIs.

c) Provide general information about risk factors to be considered by the SFIs when conducting ML/TF/PF risk identification.

d) Enable the SFIs develop policies, controls and procedures that effectively manage and mitigate the inherent risks identified by the SFIs.

e) Enable the SFIs design an effective organizational structure and governance framework to implement effective ML/TF/PF risk management controls.

f) Enable SFIs develop processes to systematically check and assess the adequacy of the control system and,

g) Enable SFIs adopt additional measures to mitigate the ML/TF/PF risk frequently.

3.2 These Guidelines are not intended to replace or contradict the Act and the Regulations. Unless otherwise stipulated under the applicable Acts and Regulations, SFIs should implement the provision of this guidance as a minimum standard for purposes of compliance with the AML/CFT Compliance Program.

4. The Purpose of ML/TF/PF Risk Assessment Guidelines

4.1 The purpose of ML/TF/PF Risk Assessment guidelines is to drive improvements in the ML/TF/PF risk management process through identifying and understanding the ML/TF risk SFIs are facing, determining how these risks are mitigated by SFIs' AML/CFT program controls and relevant measures.

4.2 In addition, these guidelines are aimed at assisting SFIs in conducting their risk assessments and applying appropriate risk management and mitigation policies, controls, and procedures, i.e. risk assessment forms the basis of a risk-based approach (RBA) to AML/CFT/CPF. RBA supports SFIs in the way they implement prevention and mitigation measures that are commensurate with the ML/TF/PF risks identified.

4.3 The results of a risk assessment can be used for several objectives, including:

a) Identifying gaps or opportunities for improvement in AML/CFT/CPF policies, procedures and processes.

b) Making informed decisions about application of appropriate risk mitigation measures commensurate with the identified risks, allocation of resources and technology spend.

c) Assisting senior management in understanding how the structure of a business unit or business line's AML/CFT/CPF compliance program aligns with its risk profile.

d) Developing risk mitigation strategies including applicable internal controls.

e) Ensuring senior management are made aware of the key risks, control gaps and remediation efforts.

f) Assisting senior management with strategic decisions in relation to commercial exits and disposals.

g) Ensuring regulators are made aware of the key risks, control gaps and remediation efforts across the SFIs; and

h) Assisting senior management in ensuring that resources and priorities are aligned with identified ML/TF/PF risks.

5. Minimum expectations relating to the ML/TF/PF Risk Assessment Methodology

5.1 SFIs are required to identify, assess, and understand the ML/TF/PF threats inherent in their business activities, the ML/TF/PF vulnerabilities in their processes, and the level of AML/CFT/CPF controls and establish the net/residual ML/TF/PF risks.

5.2 The SFI's identification and understanding of the ML/TF/PF risks, requires access to accurate, timely and objective information about ML/TF/PF risks in the country and specific to the SFI. This information may be obtained from key sources of information such as the National Risk Assessment report, typology reports from the Financial Intelligence Authority as well as other sources as indicated in Paragraph 7.5 below, publicly available information for example from FATF, Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) amongst other bodies, input from business line experts, management, compliance team, legal units together with advice from external experts if necessary. SFIs should collect and maintain granular data at onboarding stage to enable sorting natural persons, legal persons and legal arrangements by categories, business types, business sectors. Assessing the ML/TF/PF risks means SFIs should determine how the ML/TF/PF threats identified will affect them.

5.3 SFIs should determine or identify the ML/TF/PF *"threat"* by evaluating the type of customers from various Geographical perspectives that are willing to exploit the SFIs (products, services and distributions channels) based on several factors including;

a) The nature, scale, diversity, and complexity of the SFI.

b) The target markets of the SFI including retail banking, corporate and investment banking, wealth management, correspondent banking services.

c) The number of customers already identified as high-risk.

d) The jurisdictions the SFI is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organized crime, and/or deficient AML/CFT/CPF controls and listed by FATF.

e) The distribution channels, including the extent to which the SFI deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology.

f) The internal audit and regulatory findings.

g) The volume and size of its transactions, considering the usual activity of the SFI and the profile of its customers.

5.4 The SFI should analyze the vulnerabilities by evaluating the regulatory framework deficiencies, internal data quality issues or internal control weaknesses that can contribute to not sufficiently identifying the threat of ML/TF/PF.

5.5 At a minimum the SFIs should assess the ML/TF/PF threats inherent in their:

a) Customer base & types.

b) Products, services and transactions

c) Geographic areas in which they operate or where their customers are located, and

d) Delivery or distribution channels for their products, services, and transactions.

5.6 These risk factors are not exhaustive, and SFIs can assess additional risk factors depending on, among others, the risk and context of SFIs business

models. It is also not mandatory for the SFIs to adopt the methodology prescribed in these guidelines for their ML/TF/PF Risk Assessment, if the SFI's risk assessment approach performed by the SFI is reliable, relevant to their business model, coherent, consistent, transparent and understandable to both the SFI and the Supervisors. Additionally, the examples provided in these guidelines are only for illustrative purposes to enable the SFIs undertake their risk assessment.

5.7 A common approach is to assess the inherent ML/TF/PF risks related to the risk factors and the adequacy of the AML/CFT/CPF controls, based on quantitative data and qualitative information. Inherent risks cannot be mitigated entirely, and the risks that remain after AML/CFT/CPF controls have been applied are termed residual risks. The SFI should implement additional measures that are commensurate to its residual risk.

5.8 The SFIs should establish policies, procedures, and controls to mitigate the residual risks that have been identified and assessed and comply with their legal and regulatory obligations regarding AML/CFT/CPF. The measure should be proportional to and consistent with the level of risks assessed, applying enhanced measures where higher risks have been identified and applying simplified measures where risks are lower.

5.9 The SFI should at the minimum ensure that the ML/TF/PF Risk Assessments comply with the following:

a) The Risk Assessment Report is documented, indicates the key findings of the assessment, and is approved by Senior management and Board of Directors of the SFI.

b) Submit a copy of the risk assessment to Bank of Uganda and the Financial Intelligence Authority within forty-eight (48) hours days after obtaining approval by the Board of Directors.

c) Develop and implement mechanisms and systems to identify and assess the ML/TF/PF risks consistent with the nature of business and size of the SFI.

d) On account of the risk assessment:

i. Update or develop and implement policies, controls, and procedures to effectively detect, manage and mitigate the identified risks
ii. Establish a process for monitoring the implementation of policies, controls, and procedures to address the ML/TF/PF risks

e) Undertake measures to review and update the risk assessment whenever there are changes in the SFIs' business environment, such as entry into new

markets, the introduction of new products, services and technologies, changes, or emerging ML/TF/PF typologies.

6. ML/TF/PF Risk Assessment of the Business

6.1 The context risk is defined as "a function of likelihood of occurrence of risk events and the impact of the risk events". The likelihood of occurrence is a combination of threat and vulnerabilities, or in other words, risk events occur when a threat exploit vulnerability. Accordingly, the level of risks can be mitigated by reducing the size of the threats, vulnerabilities, or their impact.

6.2 In order to establish the SFIs' exposure to ML/TF/PF and how efficient the risk management, the SFIs must identify every segment of its business operations where a ML/TF threat may emerge and to assess their vulnerability to that threat. ML/TF/PF risks should be identified at all management levels, from the operational level to the board of directors, and to include all organizational units/departments of the SFIs. Business-wide risk assessments should help SFIs understand where they're exposed to ML/TF/PF risk and which areas of their business they should prioritize in the fight against ML/TF/PF.

6.3 Upon identifying the ML/TF/PF risks, the SFIs should adequately assess the risks exposure by implementing effective risk management systems, which would enable SFI to evaluate the likelihood of adverse effects arising from the risk and the potential impact of that risk on the realization of business objectives.

6.4 The process of ML/TF/PF risk assessment has four stages:

a) Identifying the area of the business operations vulnerable to ML/TF/PF.

b) Conducting an analysis to assess the likelihood (ML/TF/PF threats and vulnerable) and impact of ML/TF/PF.

c) Managing the ML/TF/PF risks by developing policies, procedures, and process; and

d) Regular monitoring and reviewing the ML/TF/PF risks.

6.5 The first stage of ML/TF/PF risk assessment is to identify the varying threat and vulnerability to ML/TF/PF which arises from customers, Transactions, Products & Services, and geographic exposures to the SFI.

6.6 In the second stage, the ML/TF/PF risks that can be encountered in an SFI should be analysed as a combination of likelihood that the risks will occur and the impact or damages if the risks occur. This impact can consist of

financial loss to the business from the crime, monetary penalties from regulatory authorities, reputational risk/damage which could potentially impact the correspondent banking relationships and other sources of income channels.

6.7 In the third stage, once the inherent risk is identified, assessed, and analysed, the SFIs should apply ML/TF/PF risk management strategies and implement policies and procedures accordingly. In addition to mitigating the inherent risk effectively, adequate systems and controls should be devised and implemented.

6.8 Finally in the fourth stage, ML/TF/PF risk policies, procedures must be monitored and reviewed regularly. An SFI can do this by developing a monitoring regime through its compliance and audit programs.

7. The dynamic nature of ML/TF/PF risks

7.1 While conducting the ML/TF/PF Risk Assessments, SFIs should be cognizant of the change in environment, its profile, jurisdictions, response to market changes internally, customer demands amongst others.

7.2 The combination of these factors makes it critical that ML/TF/PF risk model and assessments are subject to reviews. SFIs should therefore establish policies and procedures which prescribe the circumstances that should trigger a review of the risk assessment and the model. In addition, the frequency and cycle of risk assessment should be driven by the level of risk. Higher ML/TF/PF risks should lead to higher frequency/cycle of risk assessment. Nevertheless, at a minimum the SFI should review the risk assessment at least annually.

7.3 Generally, SFIs should keep their Risk Assessment and assessments of the ML/TF/PF risk associated with individual business relationships as well as of the underlying factors under review to ensure their assessment of ML/TF/PF risk remains up to date and relevant. Where the SFI is aware that a new risk has emerged, or an existing one has increased, this should be reflected in Business Risk Assessment as soon as possible.

7.4 SFIs should assess information obtained as part of their ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

7.1 SFIs should ensure that they have systems and controls in place to identify emerging ML/TF/PF risks and that they can assess these risks and, where appropriate, incorporate them into their individual and Business Risk Assessments in a timely manner. Examples of systems and controls SFIs should put in place to identify emerging risks include:

a) Processes to ensure that internal information is reviewed regularly to identify trends and emerging issues.

b) Processes to ensure that the SFI regularly reviews relevant information from sources such as:

i. The Uganda National Risk Assessment.
ii. National Risk Assessment of the jurisdiction(s) in which the SFI operates or customers of a SFI are located.
iii. Communications issued by Financial Intelligence Authority of Uganda.
iv. Guidance, circulars and other communication from the Bank of Uganda and other relevant regulatory bodies
v. Information obtained as part of the initial CDD process.
vi. Information from industry bodies.
vii. Information from international standard setting bodies such as Mutual Evaluation Reports (MERs) or thematic reviews.
viii. Changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts and looking for sanctions' regime updates.
ix. Information from international institutions and standard setting bodies relevant to ML/TF/PF risks (e.g. UN, IMF, Basel Committee on Banking Supervision-BCBS, FATF); and
x. Other credible and reliable sources that can be accessed individually or through commercially available databases or tools that are determined necessary by the SFIs on a risk-sensitive basis.

c) Processes to capture and review information on risks relating to new products.

d) Engagement with other industry representatives, competent authorities and FIA (e.g. round tables, conferences and training providers), and processes to feed back any findings to relevant staff and,

e) Establishing a culture of information sharing and strong ethics within the SFI.

8. Assessing Dynamic risks of customers

8.1 Another critical component of a risk assessment is a process for reevaluating risks and determining when a customer risk rating should be raised or lowered. SFIs should identify the key factors that should trigger such a reevaluation.

8.2 In addition to the initial assessment of the inherent risk of a customer, SFIs should consider how the customer's relationship and risk changes over time. Consideration driving a customer's risk rating includes the actual activity

that the customer conducts. For example, a customer's checking account may start out as low-risk at on-boarding, however if the subsequent transaction records show that the account is involved in a high number and volume of wires to high-risk jurisdictions, indicating abnormal behavior for this customer type, the risk level for the account may need to be raised and vice versa.

8.3 Therefore, as every SFI develops transaction history with its customers, the SFIs should consider modifying the risk rating of the customer, based on but not limited to the following factors:

a) Unusual activity, including alerts, cases, and Suspicious Activity Reports (SAR) such as significant volumes of activity where it would not be expected, such as:

i. receiving multiple deposits (e.g., cash and electronic transfers) and then engaging in large international transactions,

ii. businesses engaged in large volumes of cash when this would not typically be expected of the SFI's knowledge of a customer

b) Receipt of law enforcement inquiries, such as subpoenas.

c) Transactions that violate economic sanctions programs.

9. Assessing the inherent ML/TF/PF Risk Factors

9.1 The SFI's ML/TF/PF risk factors mentioned in part 5.5 there are at least four principal inherent risk factors: customer base/type; products, services and transactions; geographic locations; and delivery channels. Consequently, SFI's risk assessment model should assess at least the ML/TF/PF risks inherent in these factors.

9.2 A key source of information for assessing the adequacy of information used for the business wide risk assessment is information from national risk assessments, sectoral risk assessments, and ML/TF/PF typologies relating to the specific sector. The interpretive note to FATF Recommendation 10 on customer due diligence provides examples of potentially higher-risk situations with respect to customers, geography, products, transactions, services, and delivery channels.

9.3 These factors, although not exhaustive are relevant for assessing the risks of an individual customer but also for conducting a business-wide risk assessment. The following describes the main elements of each of the risk factors that should form the foundation of the business-wide risk assessment:

Customer Risk:

9.4 SFIs should assess and understand the degree of risk posed by types or categories of customers as well as by individual customers. The assessment of the risk factors used in the business-wide risk assessment is an important input in determining which customers and types of customers pose varying levels of risk (for example, low, medium, and high).

a) The following examples are indications of higher-risk customers:
   i. Business relationships that are conducted in unusual circumstances
   ii. Non-resident customers
   iii. Legal persons or arrangements that are personal asset-holding vehicles
   iv. Businesses that are cash-intensive
   v. Ownership structures that appear unusual or excessively complex given the nature of the company's business.

b) SFIs will generally identify certain categories of customers as inherently high-risk because they are prescribed by law or regulation (for example, politically exposed persons), customer risks are identified in the national risk assessment or in FIA information and typologies, or their own ML/TF/PF risk assessments identify them as high-risk. These customer categories include the following, among others:
   i. Politically exposed persons
   ii. Casinos
   iii. Non-resident entities, particularly those with connections to high-risk jurisdictions
   iv. Professionals (for example, lawyers, accountants, and trust and company service providers) acting as an introducer or intermediary on behalf of clients or groups of clients (whereby there is no direct contact with the client)
   v. High-net-worth individuals
   vi. Respondent banks from high-risk jurisdictions
   vii. Private investment or asset protection vehicles.

9.5 SFIs should not, unless prescribed by law necessarily categorize all of the persons or entities in one of these groups as automatically high-risk, as doing so may not be accurate and may cause financial exclusion. These categories concern the assessment of inherent risks. A successful customer risk assessment framework distinguishes between high-, medium-, and low-risk clients.

9.6 Generally, when identifying and assessing the inherent risk associated with customers, including customers' beneficial owners, SFIs should consider the risk related to:

a) The customer's and the customer's beneficial owner's **business or professional activity**.

b) The customer's and the customer's beneficial owner's **reputation,** if relevant to informing the SFI about the customer's or beneficial owner's financial crime risk; and

c) The customer's and the customer's beneficial owner's **nature and behavior**.

9.7.1 Customer's Business or Professional Activities

a) SFIs should consider the risk factors associated with a customer's or their beneficial owner's business or professional activity including for example (recognizing that each of these factors will not be relevant to every customer), whether the customer or its beneficial owner:

i. Has political connections, for example: the customer or its beneficial owner is a Politically Exposed Person (PEP) or has any other relevant links to a PEP; or one or more of the customer's directors are PEPs and if so, these PEPs exercise significant control over the customer or beneficial owner
ii. Has links to sectors that are commonly associated with higher corruption risks or trade-based money laundering
iii. Has links to sectors that are associated with higher ML/TF/PF risk, for example certain Money Service Businesses, casinos or dealers in precious metals.
iv. Has links to sectors that involve significant amounts of cash.
v. Is a legal person or a legal arrangement and if so, the purpose of their establishment and the nature of their business.
vi. Is a public body or state-owned entity from a jurisdiction with high levels of corruption.

b) Other risk factors that SFIs may consider in relation to a customer's business or professional activity include, for example, whether:

i. The customer is a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available. For example, a public company listed on a regulated market or other trading platform that makes such disclosure a condition for listing and/or admission to trading.
ii. The customer is a credit or financial institution acting on its own account from a jurisdiction with an effective AML/CFT/CPF regime. For example whether: It is supervised for compliance with local AML/CFT/CPF obligations; and If so supervised, there is no evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT/CPF obligations or wider conduct requirements in recent years; or
iii. The customer's background is consistent with what the SFI's knows. For example: Its former, current or planned business activity; The turnover of

the business; Its source of funds; and the customer's or beneficial owner's source of wealth.

9.7.2 Customer's Reputation

Risk factors that SFIs should consider, where appropriate, when assessing the risks associated with a customer's or their beneficial owner's reputation include, for example whether:

a) There are adverse media reports or other relevant information sources about the customer or its beneficial owner. For example, there are reliable and credible allegations of criminality or terrorism against the customer or their beneficial owners. SFIs should determine the credibility of allegations inter alia based on the quality and independence of the source data and the persistence of reporting of these allegations.

b) The customer, beneficial owner or anyone publicly known to be closely associated with them has currently, or had in the past, their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing.

c) The customer or beneficial owner has been the subject of a suspicious transactions report by the SFI in the past; or

d) The SFI has in-house information about the customer's or their beneficial owner's integrity, obtained for example, in the course of a long-standing business relationship.

9.7.3 Customer's Nature and Behavior

SFIs should consider, where appropriate, when assessing the risk associated with a customer's or their beneficial owner's nature and behavior include, consider whether:

a) The customer is unable to provide robust evidence of their identity.

b) The SFI has doubts about the veracity or accuracy of the customer's or beneficial owner's identity.

c) The customer's ownership and control structure appears unnecessarily complex or opaque and there is no obvious commercial or lawful rationale for such structures.

d) The customer is a special purpose vehicle (SPV) or structured finance company where beneficial ownership is not transparent.

e) There are frequent or unexplained changes to a customer's legal, governance or beneficial ownership structures (e.g., to its board of directors).

f) The customer requests transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without apparent economic or lawful purpose or a sound commercial rationale.

g) There are grounds to suspect that the customer is trying to evade specific thresholds such as those set out under the definition of "occasional transaction".

h) The customer's or beneficial owner's source of wealth or source of funds cannot be easily and plausibly explained.

i) The customer does not use the products and services it has taken out as expected when the business relationship was first established.

j) The customer is a non-resident, and the needs could be better serviced elsewhere.

k) The customer is a non-profit organization whose activities put them at a heightened risk of being abused for terrorist financing purposes;

Transactions, Products & Services:

9.8 SFIs should take stock of the lines of business (transactions, products and services) that are more vulnerable to ML/TF/PF abuse and how a customer uses a product or service to determines the likelihood (threats and vulnerabilities) of abuse.

9.9 Financial institutions should assess the inherent risks of abuse of products and services by customers, by considering factors such as their ease for holding and transferring value or their complexity and transparency. Not all products and services attract the same level of risk, and the model used to assess risk should evaluate their likelihood and impact for being abused for ML/ TF/PF.

9.10 To assess the degree of inherent risk, other factors should be taken into account, such as the volume of use, meaning the amount and number of accounts or transactions. The risk factor that SFIs should consider when assessing the risk associated with their products, services include, for example:

a) The **level of transparency, or opaqueness**, the product & service

b) The **complexity of the product & service**; and

c) The **value or size** of the product & service.

9.10.1 Transparency of Transactions, Products & Services

The risk factors that SFIs should consider when assessing the risk associated with the transparency of products& services include, where appropriate, for example:

a) The extent to which products or services facilitate, or allow anonymity or opaqueness of customer, ownership or beneficiary structures that could be used for illicit purposes, for example:
i. Pooled accounts, offshore and certain trusts.
ii. Legal entities structured in a way to take advantage of anonymity; and

b) The extent to which is it possible for a third party that is not part of the business relationship to give instructions, for example, certain correspondent banking relationships.

9.10.2 Complexity of Products, Services or Transactions

The risk factors that SFIs should consider when assessing the risks associated with Transactions, Products & Services include, where appropriate, for example:

a) The extent that the transaction is complex and involves multiple parties or multiple jurisdictions, for example, certain trade finance transactions.

b) Conversely, the extent that the transaction is straightforward, for example, regular payments into a pension fund.

c) The extent that the products or services allow payments from third parties or accept overpayments. Where third party payments are permitted, the extent to which:
i. The SFI can identify the third party and understands their relationship with the customer and
ii. The risks associated with new or innovative products or services, in particular where this involves the use of new technologies or payment methods.

9.10.3 Value and Size of Transactions, Products & Services

Risk factors that SFIs should consider when assessing the risk associated with the value or size of a product & services include, where appropriate, for example:
a) The extent that products or services may be cash intensive, for example, certain types of payment services and current accounts; and

b) The extent that products or services facilitate or encourage high value transactions, for example there are no caps on certain transaction values or levels of premium that could limit the use of the product or service for money laundering or terrorist financing purposes

Delivery Channel/Distribution Risk

9.11 SFIs should also assess the inherent risks associated with their business activities, processes, and transactions with respect to the delivery channels used. Inherently high-risks occur in non-face-to-face situations—especially when no safeguards are in place, such as an electronic means of identification—and when professional intermediaries and introducers are used.

9.12 The following examples as below;

a) Risk factors related to higher-risk products and services/transactions:
i. Private banking
ii. Anonymous transactions (which may include cash)
iii. Non-face-to-face business relationships or transactions (without the use of reliable, independent digital identity and other responsible innovative solutions)
iv. Payments received from unknown or unassociated third parties.

b) Risk factors of lower-risk products, services, transactions,
i. Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.
ii. Back-to-back loans
iii. Financial guarantees (for example, trade finance, stand-by letters of credit)
iv. Currency exchange

9.13 When identifying the risk associated with Delivery Channel/ Distribution, SFIs should consider the risk factors related to:

a) The extent that the business relationship is conducted on a non-face to face basis; and,

b) Any introducers or intermediaries the SFI utilizes and the nature of their relationship to the SFI.

9.13.1 How the Business Relationship is conducted

Risk factors that SFIs should consider when assessing the risk associated with how

the business relationship is conducted, include for example, whether: the customer is physically present for identification purposes. If they are not,

a) Whether the SFI uses reliable forms of non-face to face CDD; and

b) The extent that the SFI has taken steps to prevent impersonation or identity fraud.

9.13.2 Channels used to introduce customer to the SFI

Risk factors that SFIs should consider when assessing the risk associated with customers introduced to the SFIs, include for example

a) The extent that the SFI can rely on this introduction as re-assurance that the customer will not expose the SFI to excessive ML/TF/PF risk.
b) The extent that the SFI has taken measures to satisfy itself that the third-party entity applies CDD measures and keeps records equivalent to the SFI's standards.

c) The customer has been introduced from a third party, for example a bank that is not part of the same group. In such instances, whether that third party is a financial institution, or their main business activity is unrelated to financial service provision.

d) The third party will provide immediately upon request, relevant copies of the identification and verification data among others to the SFI when requested.

e) The quality of the third party's CDD measures is such that it can be relied upon.

f) A regulated person subject to AML Obligation that are consistent with the AML/CFT/CPF laws and regulations.

g) Subject to effective AML Supervision and there are indications that the intermediary's level of compliance with applicable AML legislation or regulations is adequate. E.g the intermediary has not been sanctioned for breaches of AML/CFT/CPF obligations.

h) Where an intermediary is based in a high-risk third country that has been identified as having strategic deficiencies, SFIs should not rely on the intermediary.

Country or Geographic Risk

9.14 SFIs generally have geographic ML/TF/PF risk exposure from both domestic and cross-border sources. These risks arise from the locations where the

institution has offices, branches, and subsidiaries; and locations where customers reside or conduct their activities.

9.15 SFIs can obtain information on geographic risk from national risk assessments and the Financial Intelligence Authority (FIA), the FATF list of jurisdictions with systemic deficiencies in their AML/CFT/CPF regimes (grey-list), those subject to a call of action (blacklist), among other sources, to identify high-risk regions and jurisdictions. For example, branches in border regions, airports, free trade zones, or areas with higher criminality may pose higher ML/TF/PF risks.

9.16 With regard to cross-border exposures, SFIs can also draw on the information from sources such as;
(a) Mutual evaluation reports
(b) Publications by the OECD could be relevant, for example, to identify non-cooperative or particularly opaque jurisdictions for tax purposes which pose heightened risks of tax evasion / tax crimes.
(c) The peer reviews published by the OECD on the implementation of the Anti-Bribery Convention
(d) UN. The United Nations Office on Drugs and Crimes (UNODC) carries out peer reviews on the implementation of the UN Convention against Corruption (UNCAC)

9.17 When conducting both the entity and individual risk assessment, the SFI should consider the geographic risk in combination with customer risk or product/service risk. For instance, a corporate customer may be active in or have an ultimate beneficial owner from a high-risk jurisdiction, or a customer might send funds to a high-risk jurisdiction.

9.18 The Country or Geographic risks relate to:

a) Jurisdictions in which the customer and beneficial owner is based.

b) Jurisdictions which are the customer ' s and beneficial owner's main places of business; and,

c) Jurisdictions to which the customer and beneficial owner appear to have relevant personal links, of which the Firm should reasonably have been aware.

9.19 When identifying the risk associated with countries and geographic areas, SFIs should consider for example the risk factors related to:

a) The nature and purpose of the business relationship within the jurisdiction.

b) The effectiveness of the jurisdiction's AML/CFT/CPF regime.

c) The level of predicate offences relevant to money laundering within the jurisdiction.

d) The level of ML/TF/PF risk associated with the jurisdiction.
e) Any economic or financial sanctions against a jurisdiction; and

f) The level of legal transparency and tax compliance within the jurisdiction.

9.19.1 Nature and Purpose of the Business Relationship within the Jurisdiction

The nature and purpose of the business relationship will often determine the relative importance of individual country and geographic risk factors. Risk factors SFIs should consider, where appropriate, include for example:

a) Where the funds used in the business relationship have been generated abroad, the level of predicate offences relevant to ML/TF/PF and the effectiveness of a country's legal system.

b) Where funds are received from or sent to jurisdictions where groups committing terrorist offences are known to be operating, the extent to which this is expected or might give rise to suspicion is based on what the SFI knows about the purpose and nature of the business relationship.

c) Where the customer is a financial institution, the adequacy of the country's AML/CFT/CPF regime and the effectiveness of AML/CFT/CPF supervision; or

d) For customers other than natural persons, the extent to which the country in which the customer (and where applicable, the beneficial owner/s) is registered, effectively complies with international tax transparency

9.19.2 Effectiveness of jurisdiction's AML/CFT/CPF Regime

Risk factors that SFIs should consider when assessing risk associated with the effectiveness of a jurisdiction's AML/CFT/CPF regime include for example, whether:

a) The country has been identified by the FATF as having strategic deficiencies in their AML/CFT regime as stipulated in regulation 44 on high-risk countries in the AML Regulations, 2015.

b) There is information from one or more credible and reliable sources about

the quality of the jurisdiction's AML/CFT/CPF controls including information about the quality and effectiveness of regulatory enforcement and oversight. Examples of possible sources include

i. Mutual Evaluations of the FATF and FATF style Regional Bodies
ii. The FATF's list of high-risk and non-cooperative jurisdictions
iii. International Monetary Fund 's FSAP reports and
iv. IMF Staff Reports and other relevant IMF publications.

9.19.3 Level of Jurisdiction's predicate Offences

Risk factors that the SFIs should consider when assessing the risk associated with the level of predicate offences relevant to money laundering in a jurisdiction include for example whether.

a) The information from credible and reliable public sources about the level of predicate offences relevant to money laundering, for example corruption, organized crime, tax crime or serious fraud. Examples include corruption perceptions indices, OECD, UNODC and the peer reviews carried out by the Global Forum on Transparency and Exchange of Information for Tax Purposes.

b) There is information from more than one credible and reliable source about the capacity of the jurisdictions investigative and judicial system effectively to investigate and prosecute these offences.

9.19.4 Level of Jurisdiction's TF Risk

Risk factors that SFIs should consider when assessing the level of TF risk associated with a jurisdiction include, for example, whether:

a) There is information, for example, from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory; or
b) The jurisdiction is subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued, for example, by the United Nations.

9.19.5 Level of Jurisdiction's Transparency and Tax Compliance

Risk factors that SFls should consider when assessing the jurisdiction's level of transparency and tax compliance include, for example, whether:

a) There is information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards and there is evidence

that relevant rules are effectively implemented in practice. Examples of possible sources include:

i. Reports by the OECD's Global Forum on Transparency and the Exchange of Information for Tax Purposes, which rate jurisdictions for tax transparency and information sharing purposes.
ii. Assessments by the FATF of the jurisdiction's compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5; or
iii. IMF staff assessments of Offshore Financial Centres).

b) The jurisdiction is committed to, and has effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014; and

c) The jurisdiction has put in place reliable and accessible beneficial ownership registers.

9.20 Other Relevant Factors: SFIs should also consider factors that may present specific or ancillary risks. These factors can include the following:

a) Introduction of new products or services, new technologies, or delivery processes.

b) Establishment of new branches and subsidiaries locally and abroad.

c) Unusually high growth or disproportionately large share of profits from a certain branch or subsidiary.

d) Mergers and acquisitions of businesses.

e) Significant growth in high-risk products or services.
f) New typologies on ML/TF/PF.

g) Changes in AML/CFT/CPF laws, regulations, and guidelines.

h) High staff turnover in high-risk business lines and compliance.

i) ML/TF/PF investigations or legal and regulatory action affecting the institution.

10.20 The criteria used to apply each country with their risk ratings indicating examples of country/geographic risk is indicated in Annex 3.

11.20 Frequency of reviewing and updating the country/Geographic risk ratings aligned to some of the relevant release dates of the source information. If new sanctions are imposed, then the rating will be updated as and when that occurs.

10. Assessing the level of the ML/TF/PF risk

SFIs should take a holistic view of the ML/TF/PF risk factors they have identified that, together, will determine the level of ML/TF/PF risk associated with a business relationship or transaction.

10.1 Weighting Risk Factors As part of this assessment

a) SFIs should consider whether to weight risk factors differently depending on their relative importance. When weighting risk factors, SFIs should make an informed judgment about the relevance of different risk factors in the context of a business relationship or transaction.

b) The weight given to each of these risks factors is likely to vary from product to product and customer to customer (or category of customer) and from one SFI to another. When weighting risk factors SFIs should ensure that:

i. Weighting is not unduly influenced by just one risk factor.
ii. Economic or profit considerations do not influence the risk rating.
iii. Weighting does not lead to a situation where it is impossible for any business relationship to be classified as high-risk;
iv. Situations identified by AMLA as always presenting a high ML/TF/PF risk cannot be over-ruled by the SFI's weighting, for example politically exposed persons and correspondent banking must apply enhanced customer due diligence; and
v. SFIs are able to override any automatically generated risk scores where necessary and the overriding process should also be guided by adequate policies and procedures. The rationale for the decision to override such scores should be governed and documented appropriately and must be subjected to periodic process of reviewing the overall effectiveness of the model.

c) Where an SFI uses automated IT systems to allocate overall risk scores to categorize business relationships or transactions and does not develop these in house, rather purchases them from an external provider, they should ensure that:

i. The SFI fully understands the risk rating methodology and how it combines risk factors to achieve an overall risk score.
ii. The methodology used meets the SFI's risk assessment requirements and AML/CFT/CPF obligations;
iii. The SFI is able to satisfy itself that the scores allocated are accurate and reflect the SFI's understanding of ML/TF/PF risk and
iv. The overall effectiveness of the model is subjected to periodic process of reviewing.

10.2 Categorizing business relationships and occasional transactions

a) Following their risk assessment, SFls should categorize their business relationships and occasional transactions according to the perceived level of ML/TF/PF risk.

b) SFls should decide on the most appropriate way to categorize risk. This will depend on the nature and size of the SFl's business and the types of ML/TF/PF risk to which it is exposed. The steps SFls take to identify and assess ML/TF risk across their business should be proportionate to their nature and size.

10.3 Hypothetical Case of Risk Assessment Process

The hypothetical examples of the Risk assessment model have been provided in Annexes for purposes of Illustration only. The hypothetical model is not provided for SFIs to implement but rather demonstrate a typical process which would be undertaken to conduct a risk assessment. SFIs should develop their own risk assessment model and framework suitable to their institution.

11. Risk Mitigation

11.1 The ML/TF/PF risk assessment provides the foundation for the SFI to develop an effective and proportionate AML/CFT/CPF framework. This framework includes AML/CFT/CPF policies, procedures, and controls to mitigate inherent risks as well as institution-wide vulnerabilities.

11.2 SFIs should enhance the mitigation measures for high-risk scenarios, while less rigorous controls can be applied to low-risk scenarios. Standard controls should apply in the areas or scenarios that are identified as medium risk. The following are some of the building blocks for an effective AML/CFT/CPF framework.

Governance Arrangements:

11.3 An effective risk-based approach to AML/CFT/CPF Program requires a Board of Directors and Senior Management that are committed to lead and oversee its development and implementation. This includes having an approach to AML/CFT/CPF compliance that considers the legislative obligations as the starting for AML/CFT/CPF Program. SFIs should engage with the Central Bank in a positive, transparent way and should be proactive in bringing matters to the attention of the Central Bank. This commitment requires the following actions:

a) Fostering a culture of compliance as a core value of the SFI that focuses on intrinsic motivation to control ML/TF/PF risks by establishing an effective

communication system to inform staff of ML/TF/PF risks and (changes to) the AML/CFT/CPF policy and related matters.

b) The SFIs should ensure that the Board of Directors have a clear understanding of ML/TF/PF risks. The information about ML/TF/PF risk assessment should be communicated to the Board in a timely, complete, understandable and accurate manner so that it is equipped to make informed decisions.

c) Approve and oversee the implementation of the AML/CFT/CPF policies, procedures, and controls adapted to the SFI's ML/TF/PF risk profile and regulatory environment.

d) According to the BOU Corporate Governance Guidelines (October 2022), SFIs should establish transparent and effective governance and management information systems that keep the Board and Senior management informed of ML/TF/PF risks, emerging threats and trends, and compliance issues, such as statistics on unusual and suspicious transactions, regulatory measures, and sanctions in a timely manner.

e) Explicit responsibility should be allocated by the board of directors effectively taking into consideration the governance structure of the SFI for ensuring that the policies and procedures are managed effectively for example designating a Board Committee to be responsible for AML/CFT/CPF compliance and ML/TF/PF risks as well as appointing a Money Laundering Control Officer (MLCO)[2] at Senior Management level.

f) Allocating adequate resources for the main control functions of the institution, especially compliance and internal audits, to enable the board to monitor the effective implementation of the AML/CFT/CPF framework.

g) Having a sufficient budget and resources for AML/CFT/CPF, including staff training, software, and equipment.

The role of the Board and Senior Management

11.4 SFIs should ensure that there is appropriate governance and oversight with regard to its compliance with obligations under the AMLA and ATA laws and regulations. Therefore, at the SFIs should ensure that:

a) The Risk Assessments:

[2] The Money Laundering Control Officer should at a minimum have overall responsibility for the AML/CFT function with the stature and the necessary authority within the SFI such that issues raised by this Senior Officer receive the necessary attention from the Board, Senior Management and Business lines.

i. Senior Management has reviewed and approved the methodology used for undertaking the SFI's Risk Assessment.
ii. Senior Management has reviewed and approved the SFI's Risk Assessment at least on an annual basis to ensure that it is aware of the ML/TF/PF risks facing the SFI and that the corresponding AML/CFT/CPF measures which the Firm has in place are appropriate for the level of ML/TF/PF risk identified

b) Policies and Procedures
i. The board approved all written policies.
ii. Senior Management has reviewed and approved all processes, procedures, and material updates.

c) Reporting Lines:
i. Appropriate reporting lines are in place to facilitate the escalation of AML/CFT/CPF issues from the MLCO for discussion at Senior Management level.

d) Senior Management Meetings:
i. AML/CFT/CPF issues appear as an agenda item at regular intervals at Senior Management meeting(s) and that the corresponding minutes reflect the level of discussion and outcomes, which took place concerning any Management Information (MI) provided by the MLCO or any particular AML/CFT/CPF issues requiring discussion by the Senior Management.
ii. The MLCO delivers a report to the board or a board committee at quarterly and that a detailed discussion on its content takes place with a corresponding minute to reflect the level of discussion.
iii. SFIs should ensure that appropriate evidence of discussions at Senior Management meetings and/or approvals concerning AML/CFT/CPF issues are recorded and retained in accordance with the SFI's record retention policy.

e) AML/CFT/CPF Resourcing
i. The SFI's AML/CFT/CPF function is adequately resourced (both in terms of staff and systems) commensurate with the level of ML/TF/PF risk faced by the Firm.
ii. Reviews are undertaken on a regular and timely basis to consider whether the SFI has the appropriate staff numbers, the correct skill-set and whether staff have access to adequate systems and other resources to effectively perform their role as it relates to AML/CFT/CPF issues.

The three Lines of Defence Model for ML/TF/PF Risk management

11.5 SFIs should implement a "three lines of defence" model to manage and oversee ML/TF/PF risks. Accordingly, SFIs should ensure that there is adequate and effective co-ordination between the front-line business unit,

risk, compliance and internal audit, or equivalent to ensure robust and well-structured oversight, as well as effective co-ordination of resources to manage overlap in areas of review.

11.6 In the context of AML/CFT/CPF, SFIs should apply the risk management concept of the three (03) lines of defence as follows.

a) The business units (e.g. front office, customer facing activity) are the first line of defence in charge of identifying, assessing and controlling the risks of their business. They should know and carry out the policies and procedures and be allotted sufficient resources to do this effectively.

b) The second line of defence includes the Money Laundering Control Officer (MLCO) or the Senior Manager in charge of the AML/CFT/CPF Compliance Program/function but also human resources or technology.

c) The third line of defence is ensured by the internal audit function or an independent review by an external AML/CFT /CPF expert.

11.7 ***The first line of defence,***

a) SFIs should ensure that AML/CFT/CPF policies and procedures are clearly specified in writing and communicated to all personnel. The policies and procedures should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the SFI in compliance with AML laws and regulations.

b) SFIs should establish internal procedures for detecting and reporting suspicious transactions. There should be adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards.

11.7.1 ***AML/CFT/CPF Training Programs***

a) SFIs should implement ongoing employee training programs so that staff are adequately trained to implement the bank's AML/CFT/CPF policies and procedures. At the minimum the training program should:

i. Establish the components of the training which should be in line with the training requirement stipulated in Section 6 (17) - (d) of the AMLA Act (as amended) 2017 and Regulations 11 (d) & (e) & 32 (2) of the Anti-Money Laundering Regulations 2015.

ii. The timing and content of training for various sectors of staff should be adapted by the SFI according to their needs and the SFI's risk profile.

iii. Training needs should be tailored depending on staff functions and job responsibilities and length of service with the bank. The Training course content and materials should be tailored to an employee's specific

responsibility or function to ensure that the employee has sufficient knowledge and information to effectively implement the SFI's AML/CFT/CPF policies and procedures.

iv. Obligatory to all staff, hence new employees should be required to attend training as soon as possible after being hired.

v. Refresher training should be provided to ensure that staff are reminded of their obligations and their knowledge and expertise are kept up to date.

vi. The scope and frequency of such training should be tailored to the risk factors to which employees are exposed due to their responsibilities and the level and nature of risk present in the bank.

b) An effective training program should not only explain the relevant AML/CFT/CPF laws and regulations, but also cover the SFI's policies and procedures used to mitigate ML/TF/PF risks, significant AML/CFT/CPF non-compliance issues raised by the Regulator or the external reviews (e.g. internal or external audits). Training should include both formal training courses and ongoing communications that serve to educate employees and maintain their ongoing awareness about AML/CFT/CPF requirements, such as emails, newsletters, periodic team meetings, intranet sites, and other means of sharing information.

c) SFIs should periodically identify the target staff/employees to be trained according to the approved annual training plan. In particular, new staff members or staff transferring to new roles should receive training during employee orientation or shortly thereafter (within a defined period in the policies or procedures manual).

d) SFIs should establish a program which identifies and implement training sessions for situations that demand an immediate training or enhanced training beyond the basic training program. For example, an urgent or adhoc training session might be necessary right after an examination or audit that uncovers serious AML/CFT/CPF control deficiencies, a news story that names the SFI, or recent regulatory action, such as a consent order, which might also prompt quick-response training. Changes in software, systems, procedures, and regulations are additional triggers for training sessions, as well as specific money laundering or other illicit financial activity risks that impact a specific business line or department of the SFI.

e) Each segment of the staff should be trained on AML/CFT/CPF topics and issues that are relevant to their activities. The training scope should at least cover the following:

i. ***Customer-facing staff who are the SFI's first line of defense.*** These employees require the deepest practical understanding of why AML/CFT/CPF efforts are important and what they need to do to be vigilant about ML/TF/PF risk. Their training should include both

general importance of AML/CFT/CPF and, additional training on specific unit procedures related to the products and services carried out by the business lines. For example, loans, credit, and loan-operations staff need training on how money launderers might misuse credit products, how the staff can recognize potential money laundering, and what the staff must do if they see it. Cash handlers often need special training because many jurisdictions have imposed additional requirements to address the increased risk posed by cash. These employees need to know how to properly handle cash transactions, especially those that trigger reporting requirements, including when to escalate concerns when a customer attempts to structure a transaction to avoid the reporting requirements. Employees who establish loans and accounts for new customers need to know applicable regulatory requirements and the organization's policies and procedures for identification and performing due diligence during the onboarding process.

ii. ***Operations personnel:*** Non-customer-facing employees with the SFI's lines of business are also included in the first line of defense and should obtain specialized trainings relevant to their job roles. For example, cash vault, wire transfer, trade finance, loan underwriters, loan collections, and treasury management personnel should be in position to recognize illegal, fraudulent, and unusual account activity. Therefore, SFI should ensure that specialized training for these individuals to recognize AML/CFT/CPF red flags and elevate unusual activity to compliance personnel should be considered.

iii. ***AML/CFT/CPF Compliance staff:*** Under the direction of a designated compliance officer, the compliance staff function coordinates and monitors the SFI's day-to-day AML/CFT/CPF compliance program. Given this area's responsibility for managing the organization's adherence to AML/CFT/CPF regulations, more advanced ongoing training to stay abreast of requirements and emerging trends is important.

iv. ***Independent testing staff (Internal Audit function Staff):*** Independent testing personnel independently assesses the adequacy of the AML/CFT/CPF compliance program; therefore these employees should receive periodic training concerning regulatory requirements, changes in regulation, money laundering methods and enforcement, and their impact on the SFI.

v. ***Senior management and Board of Directors:*** The Board and Senior Management specialized training should address the importance of AML/CFT/CPF regulatory requirements, regulatory changes that impact the SFI, penalties for non-compliance, personal liability, and

the SFI's unique risks. Without a general understanding of this information, Senior Management and the Board of Directors may not adequately provide for AML/CFT/CPF oversight, approve AML/CFT/CPF policies, and provide sufficient resources.

f) Training best practices include the following:
   i. Appropriate training tailored to the individual's Staff specific roles.
   ii. Generic training is acceptable, provided it is supplemented with specific training with a practical application to the specific line of business or role within the SFI.
   iii. Periodic refresher training—usually annually—is important for existing employees.
   iv. SFIs should assess whether third parties and employees working in outsourced functions need to attend specific AML/CFT/CPF training.

11.8 *The second line of defense*

a) The SFI's compliance function constitutes the second line of defense. It is responsible for monitoring the controls of the business, which is the first line of defense. Regardless of the structure, the role of the second line of defense must be established in a manner that ensures it can fulfill its role effectively. The sophistication of the compliance function should be based on the SFI's nature, size, complexity and the specific risks associated with its products, services, customers, geographical locations and delivery channels.

b) As stipulated in Regulation 6 of the AML Regulations 2015, the SFI should appoint the Money Laundering Control Officer (MLCO). SFIs should there ensure that the appointing of the MLCO is approved by the Board of Directors. The individual is responsible for managing all aspects of the AML/CFT/CPF compliance program. This includes, but is not limited to, designing and implementing the program, making necessary changes and updates, disseminating information about the program's successes and failures to key staff members, constructing AML/CFT/CPF-related content for staff training programs, and managing the SFI's adherence to applicable AML/CFT/CPF laws and regulations, including staying current on legal and regulatory developments in the field.

c) The MLCO should be capable of articulating matters of importance to Senior Management, particularly significant changes that could present risk to the SFI, such as a sudden or substantial increase in STRs or currency transaction reports (CTRs). Other items of concern that should be escalated to management include changes to laws and regulations that might require immediate action.

d) The MLCO must also have an indirect reporting line to the Board or an equivalent body and a direct reporting line to the Chief Executive Officer or

Executive Director. This unfettered access to board members allows him or her to undertake this oversight role in an effective manner.

e) The broad roles of the MLCO are stipulated in Regulation 7 (1) of the AML (Regulations) 2015. The SFIs should therefore prescribe the tasks and responsibilities of the MLCO regarding AML/CFT/CPF which include:

i. Managing and coordinating regulatory examinations. The MLCO should be the contact point regarding all AML/CFT/CPF issues for internal and external authorities, including the Bank of Uganda.
ii. Developing and implementing systems, mechanisms and procedures to ensure that the staff of the SFI immediately report any suspicious money laundering or financing of terrorism activity.
iii. Notifying the Financial Intelligence Authority, on behalf of the accountable person, of any suspicious money laundering or financing of terrorism activity
iv. Performing periodic reviews and updates of the AML/CFT/CPF program
v. Coordinating the implementation activities with the lines of business and support groups to ensure that applicable business procedures are updated to incorporate AML/CFT/CPF program changes
vi. Monitoring regulatory environment for changes to the program
vii. Preparing training materials and provides guidance and advice on complicated AML/CFT/CPF issues not addressed by the line of business support group
viii. Managing sanctions screening software applications and processes
ix. Monitoring and reconciling the data being received from the source systems
x. Fine-tuning the filter thresholds according to changes in the risk profile of the organization
xi. Reviewing suspected matches and reports valid matches to the appropriate regulatory authorities.
xii. Managing transaction monitoring software applications
xiii. Monitoring and reconciling the data being received from the source systems
xiv. Fine-tuning the filter thresholds according to changes in the risk profile of the SFI
xv. Participating in the design of transaction monitoring typologies and maintains the extensive documentation required
xvi. Monitoring alerts generated on customer transactions, such as those from automated systems and referrals from line-of-business staff.
xvii. Investigating alerts and referrals

f) The business interests of the SFI should not be opposed to the effective discharge of the above-mentioned responsibilities of the MLCO, the SFIs should avoid potential conflict of interest. Therefore, to enable unbiased judgments and facilitate impartial advice to management, the MLCO should not have business line responsibilities and should not be entrusted with

responsibilities in the context of data protection or the function of internal audit. Where any conflicts between business lines and the responsibilities of the MLCO arise, procedures should be in place to ensure AML/CFT/CPF concerns are objectively considered at the highest level.

g) The MLCO should have the necessary independence, authority, resources (including information technology tools), and expertise to carry out these functions effectively, as well as unrestricted access to all relevant internal information, including information from (foreign) branches and subsidiaries.

11.9 ***Internal audit Functions and the third line of defence,***

a) The SFI's Internal Audit plays an important role in independently evaluating the risk management and controls and discharges its responsibility to the Audit Committee of the Board of Directors through periodic evaluations of the effectiveness of compliance with AML/CFT/CPF policies and procedures.

b) SFIs should establish policies for conducting audits of
   i. the adequacy of the SFI's AML/CFT/CPF policies and procedures in addressing identified risks,
   ii. the effectiveness of SFI's staff in implementing the bank's policies and procedures;
   iii. the effectiveness of compliance oversight and quality control including parameters of criteria for automatic alerts; and
   iv. the effectiveness of the SFI's training of relevant personnel.

c) The Board of Directors of the SFI should ensure that audit functions are allocated staff that are knowledgeable and have the appropriate expertise to conduct such AML/CFT/CPF Audits.

d) The Head of Internal Audit Function should ensure that the audit scope and methodology are appropriate for the SFI's risk profile and that the frequency of such audits is also based on risk.

e) Periodically, internal auditors should conduct AML/CFT/CPF audits on a bank-wide basis by reviewing the effectiveness of compliance measures across all business lines, branches, and subsidiaries, both domestically and abroad if applicable.

f) In addition, internal auditors should be proactive in following up their findings and recommendations. Generally, the processes used in auditing should be consistent with internal audit's broader audit mandate, subject to any prescribed auditing requirements applicable to AML/CFT /CPF measures.

11.10 ***Policies, Procedures and Controls***

a) SFIs should implement risk-based policies, procedures, and controls to mitigate ML/TF/PF risks that they have identified and assessed with respect to their customers, products, services, transactions, geographic locations, and delivery channels.

b) AML/CFT/CPF risk management requires a comprehensive set of policies, procedures, and controls. For this reason, the standard on customer due diligence is one of the most comprehensive and important preventive measures in AML/CFT/CPF mitigation processes. The Bank of Uganda Customer Due Diligence Guidance notes (September 2022) provides guidance to SFIs on the management of ML/TF/PF risks, including with respect to a customer acceptance policy, customer and beneficial owner identification, verification and risk profiling, and ongoing monitoring.

c) The following are some of the main risk-based policies, procedures, and controls that SFI should implement to mitigate inherent ML/TF risks with respect to the above-mentioned risk factors.

i. Customer Due Diligence policies, procedures, to enable financial institutions to obtain and verify information proportionate to the risks that customers represent to the financial institution and in accordance with regulatory requirements.
ii. Ongoing Due Diligence depending on the risk profile of the customer, to enable SFIs to determine whether transactions or patterns of transactions are consistent with the institution's knowledge of the customer, its business or activities, and its initial risk profile.
iii. Conduct enhanced due diligence for cases that are rated high-risk.
iv. Record Keeping for at least ten (10) years, all of the necessary records on transactions, both domestic and international, to enable SFI to comply swiftly with information requests from the competent authorities.
v. Ongoing Monitoring and Reporting of Suspicious Transactions and Activities.

d) The AML/CFT/CPF policies, procedures and controls compliance program should be in writing and include policies, procedures, and controls that are designed to prevent, detect, and deter money laundering and terrorist financing, including how the SFI will:

i. Identify high-risk operations (products, services, delivery channels, customers, and geographic locations/jurisdictions).
ii. Periodically update its risk profile and provide for an AML/CFT/CPF compliance program tailored to manage risks.
iii. Inform the board of directors (or a committee of the board) and senior management of compliance initiatives, known compliance deficiencies, STR/SARs filed, and corrective actions taken.
iv. Develop and maintain a system of metrics reporting that provides accurate and timely information on the status of the AML/CFT/CPF program, including statistics on key elements of the program, such as the

number of transactions monitored, alerts generated, cases created, and SARs filed.

v. Assign clear accountability to people for performance of duties under the AML/CFT/CPF program.

vi. Provide for program continuity, despite changes in management, employee composition, or structure.

vii. Meet all regulatory requirements and recommendations for AML/CFT/CPF compliance.

viii. Provide for periodic review and timely updates to implement changes in regulations, at least on an annual basis.

ix. Implement risk based CDD policies, procedures, and processes.

x. Provide for dual controls and segregation of duties.

xi. Comply with all recordkeeping requirements, including retention and retrieval of records.

xii. Provide sufficient controls and monitoring systems for the timely detection and reporting of potentially suspicious activity and large transaction reporting. This should also include a procedure for recording the rationale for not reporting activity because of the findings of any investigation.

xiii. Establish clear accountability lines and responsibilities to ensure that there is appropriate and effective oversight of staff who engage in activities that might pose an AML/CFT/CPF risk.

xiv. Establish training requirements and standards to ensure that employees are made aware of and have a working understanding of the procedures to be followed and their relevance to mitigating ML/FT/PF/PF risks in their departments or areas of responsibilities.

xv. Clearly explain the importance of reporting suspicious activity, including describing how and to whom concerns should be raised, the role of the MLCO, and what the "tipping off" restriction means in practice.

xvi. Incorporate into all job descriptions and performance review processes the requirement to always comply with AML/CFT/CPF policies and procedures. Non-compliance should be addressed in accordance with existing disciplinary processes.

xvii. Develop and implement screening programs to ensure high standards when hiring employees. Implement appropriate disciplinary actions for employees who consistently fail to perform in accordance with an AML/CFT/CPF framework.

xviii. Develop and implement quality assurance testing programs to assess the effectiveness of the AML/CFT/CPF program's implementation and execution of its requirements. This is separate from the independent audit requirement, but it serves a similar purpose—to assess the ongoing effectiveness of the program.

Highlights of and Differences between AML/CFT/CPF Policies, Procedures, and Controls

Policies	i. Clear and simple high-level statements that are uniform across the entire organization (set the tone from the top). ii. Approved by Senior management and Board of Directors. iii. Reflect the high-level responsibilities of the stakeholders throughout the SFI.
Procedures	i. Translate the AML/CFT/CPF policies into an acceptable and workable practice, tasking the stakeholders with their respective responsibilities. ii. The instructions for how the SFI wants something done. iii. Typically established at the operational (not executive) level of the financial institution. iv. Much more detailed than AML/CFT/CPF policies. v. Reviewed and updated regularly.
Controls	i. The internal technology or tools the financial organization uses to ensure the AML/CFT/CPF program is functioning as intended and within predefined parameters. ii. Alert compliance department to potential outliers and deviations from normal policy that may need to be reviewed. iii. Includes management reports, automated review systems, and the utilization of multiple reviewers.

11.11 ***Ongoing Monitoring and Reporting of Suspicious Transactions and Activities***

a) SFIs should report suspicions of ML/TF/PF promptly, including attempted transactions to the FIA. This is one of the main obligations of SFIs. SFI's role in reporting useful financial intelligence to combat ML/TF/PF and related predicate offenses is a critical component of the crime-fighting activities of law enforcement and judicial authorities.

b) As per the BOU STR/SAR Guidelines (September 2022), the transaction-monitoring process constitutes an essential element in detecting and investigating possible unusual or suspicious transactions and the eventual reporting of STR/SARs to the FIA. When setting up a transaction-monitoring process and system, at a minimum the following conditions apply:

i. The transaction-monitoring process should reflect the ML/TF/PF risks identified in the business-wide risk assessment.
ii. The transaction-monitoring policy should be elaborated in the underlying procedures and processes.
iii. The transaction-monitoring system should vary depending on the nature and size of the organization and its risk profile. SFIs should adopt an automated solution for monitoring transactions, especially where the volume of transactions would make manual monitoring impossible.
iv. Where an automated transaction-monitoring system is used, it should incorporate substantiated and adequate business rules (detection rules with scenarios and thresholds). These business rules should be tested periodically for effectiveness.
v. For manual screening, especially got transaction activities, staff undertaking these tasks should have sufficient expertise to identify suspicious activity in line with the business-wide risk assessment.
vi. A clearly described process is needed for handling alerts. Investigations of alerts must be documented properly, including the decision to close the alert or to report the transaction to the FIA. Information on alerts should inform the ongoing risk assessment of customers. Even when it does not generate new alerts, transaction monitoring can help to identify patterns that can inform new typologies.
vii. The governance with respect to monitoring transactions and reporting suspicious transactions should be structured so that duties are allocated clearly and segregated.
viii. Tailored training programs should allow staff, based on their functions, to identify unusual and suspicious transactions and activities.
ix. The transaction-monitoring systems should be set up so that aggregate customer information can be monitored on a consolidated basis across business lines, branches, and subsidiaries. With respect to operations abroad, the head office should be able to implement the transaction-monitoring system in those jurisdictions and to obtain information on unusual or suspicious transactions and activities detected, subject to local laws and regulations.

12. Review of the Risk Assessment Guidelines

SFIs should ensure full compliance with this Risk Assessment Guidelines and are advised to compile and record any comments, which arise in relation to implementation of these guidelines for appropriate action.

The comments should be forwarded to:

The Office of the Executive Director,
Supervision Directorate,
Bank of Uganda,
3rd Floor Plot 45,

Kampala Road, Kampala,
Uganda

ANNEXES

Annex 1: Legislative and FATF References

Legislative Reference	
Section 6A of the AMLA (as amended) 2022.	(1) An accountable person shall take appropriate steps to identify, assess and monitor its money laundering, terrorism financing and proliferation financing risks.
Section 6A (2) of the AMLA (as amended) 2022.	(2) An accountable person shall identify, assess and, take appropriate measures to manage and mitigate the money laundering, terrorism financing and proliferation financing risks that may arise in relation to— (a) the development of new products and new business practices; including new delivery mechanisms for products and services; and (b) the use of new or developing technologies for both new and pre-existing products.
Regulation 8 (1) of the AML (Regulations), 2015.	(1) An accountable person shall, on a regular basis, conduct anti-money laundering and terrorism financing risk assessment to enable the accountable person to identify, assess, monitor, manage and mitigate the risks associated with money laundering and terrorism financing, taking into account all relevant risk factors.
Section 6A (3) of the AMLA (as amended) 2017.	(3) The risk assessment under Section 6A (2) shall take place prior to the launch of the new product or business practice, or the use of a new or developing technology."
Regulations 9 (2) of the AML (Regulations), 2015.	(2) Without limiting the general effect of sub-regulation (1), an accountable person shall conduct anti-money laundering and terrorism financing risk assessment prior to the introduction of— (a) a new product; (b) a new business practice including a new delivery mechanism in relation to a product or service; (c) a new technology for both new and pre-existing products or services.
Section 6 (27) of the AMLA (as amended) 2017	A competent authority (including BOU) shall establish guidelines to assist accountable persons to implement and comply with the anti-money laundering and combatting of terrorism requirements under this Act.

Section 6 (17) (d) of the AMLA Act (as amended) 2017	(17) The SFI shall develop and implement programs for the prevention of money laundering and terrorism financing that are appropriate to the risks and the size of the accountable person's business and the programs shall include; (d) an employee training program to ensure that employees, managers and directors are kept informed of all the aspects of the anti-money laundering and combating terrorism financing requirements, new developments, money laundering and terrorism financing techniques, methods and trends, and concerning due diligence measures and suspicious transaction reporting;
Regulations 11 (d) & (e) of the AML Regulations 2015	(1) The SFI shall develop, adopt and implement internal control measures, policies and procedures for the prevention of money laundering and financing of terrorism including. (d) training programmes for the purposes of continuous training of employees, managers and directors of the accountable person, so as keep those persons up to date in all aspects of anti-money laundering and combating of terrorism financing requirements including any new developments, methods and trends concerning due diligence measures and suspicious transactions reporting systems; (e) awareness programmes for the purposes of ensuring that employees, managers and directors of the accountable person are sufficiently knowledgeable about— (i) the procedures relating to combating of terrorism and terrorism financing; (ii) the provisions of the Act and these Regulations; (iii) any policies, directives, codes or guidelines issued by the accountable person relating to anti-money laundering and combating of terrorism financing;
Regulations 32 (2) of the AML Regulations 2015	(2) The SFI shall have procedures and guidelines explaining the customer acceptance policy which forms part of the training programme of the SFI.

FATF References

FATF Immediate Outcome 4	SFIs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.
FATF Recommendation 1	Assessing risks and applying a risk-based approach

FATF Recommendation 1.10	SFIs should be required to take appropriate steps to identify, assess, and understand their ML/TF risks (for customers, countries, or geographic areas; and products, services, transactions or delivery channels)9. This includes being required to: (a) document their risk assessments. (b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied; (c) keep these assessments up to date; and (d) have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs.
FATF Recommendation 1.11	Financial institutions should be required to: (a) have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified (either by the country or by the financial institution (b) monitor the implementation of those controls and to enhance them if necessary; and (c) take enhanced measures to manage and mitigate the risks where higher risks are identified.
FATF Recommendation 10.17	Financial institutions should be required to perform enhanced due diligence where the ML/TF risks are higher.
FATF Recommendation 10.18	Financial institutions may only be permitted to apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the financial institution. The simplified measures should be commensurate with the lower risk factors but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.
FATF Recommendation 15.2	Financial institutions should be required to: (a) undertake the risk assessments prior to the launch or use of such products, practices and technologies; and (b) take appropriate measures to manage and mitigate the risks.
FATF Recommendation 15.3(c)	

VASPs are required to take appropriate steps to identify, assess, manage and mitigate their money laundering and terrorist financing risks

Annex 2: Simplified Demonstration of Risk Assessment Process

1. The following example illustrates a basic model for analyzing the inherent ML/TF/PF risk factors. The application of weights (Risk Score) is optional, and the specific weights used in Table 1 are illustrative only. Each SFI will determine whether weights (or other analytical methods) are to be applied and, if so, what weights are appropriate to use for each inherent risk factor and risks mitigating measures. The SFIs should obtain the inherent risk data from the IT Department or bank statistical data base to enable analysing the identified inherent risk parameters.

Table 1: Example of Risk Score for Inherent Risk and Risk Mitigating Measures

Inherent Risk Score	Score
Low	1
Medium -Low	2
Medium – High	3
High	4

Risk Mitigation Measures	
Strong	1
Moderate	2
Needs Improvement	3
Weak	4

2. For each data point, a rating will be given on the likelihood (supported by a threshold for example) that ML/TF/PF risks with respect to specific risk parameter will occur. As indicated in **Table 1,** risk scores, ranging from (1) to (4) are generally used. When scoring the risk parameter in for each risk factor. For example, SFIs with a large number of foreign residents and using complex legal structures and transactions in high-risk countries (either absolute or relative terms) would get a score for 4 for customer risk; Delivery Channel with a high number and number of transactions or presence of intermediaries in high-risk jurisdictions would also get inherent risk score of 4. After assessing every data point, an average rating is computed for each of the risk factors and the average of the ratings of all risk factors will be the inherent risk rating for an SFI (risk mitigation as applicable).

3. Additionally, the inherent risk rating can also be calculated by giving weights to the **risk factors.** Using a weighted approach allows the SFI to take into

account the fact that some risk factors can be more relevant to the SFI than others. The weights assigned in **Table 2** are indicative only; they can be adjusted depending on the circumstances of SFI. In this example, the total weighted inherent risk rating would be **2.25 (medium-high**); if a simple average is used, the rating would be 2.0 (medium-low).

Table 2: Example of Risk Rating for Inherent Risk Factors

Inherent risk factor	**Weight (% Optional)**	**Average* Rating**	**Weighted Rating**
Customer Type	40	3	1.2
Products & Services	20	2	0.4
Geographical Risk	25	2	0.5
Delivery Channel	15	1	0.15
Total Average	100	2	2.25

**Each risk factor may have several risk parameters (sub risk factors) hence the need to obtain the "Average Rating".*

4. The SFI can complement the quantitative approach by also using a **qualitative approach** to assess risk factors **Table 3.** SFI should not solely use the qualitative approach to assess inherent risk factors. Additionally, while in theory risk assessment can also take into account the **impact of risk** on an SFI's operations, doing so is not recommended for the simple fact that, unlike financial risks, the impact of an inherent ML/TF/PF risk that materializes is difficult to quantify and measure with any degree of precision.

Table 3: Example of Qualitative Assessment of Inherent Risk

Type of Risk	**1.Low**	**2.Medium - Low**	**3.Medium - High**	**4. High**
Type of customers	The SFI has **only** low-risk types of customers.	The SFI has **mainly** low-risk types of customers.	The SFI has **some** high-risk types of customers.	The SFI has a **significant** number of high-risk types of customers
Products and services	The SFI offers **only** low-risk products and services.	The SFI offers **mainly** low-risk products and services.	The SFI offers **some** high-risk products and services.	The SFI offers a **significant** number (or percentage) of high-risk products and services
Delivery channels	The SFI only offers	The SFI offers products and	The SFI offers products and	The SFI offers a

	products and services through direct client contact.	services mainly through direct client contact and limited non-face-to-face channels.	services through direct client contact but also substantially through non-face-to-face channels.	significant percentage of products and services through high-risk delivery channels.
Geography	The SFI has only a domestic presence and activities.	The SFI has mainly a domestic presence and very limited cross-border activities.	The SFI has a domestic as well as an international presence. Some activities take place in high-risk jurisdictions	The SFI has a large number of subsidiaries, branches, or activities in high-risk jurisdictions.

5. Similar to the inherent risk factors, all elements of the mitigating measures need to be rated. A scale of 4 qualitative ratings (strong, satisfactory, inadequate, and weak) is expedient, SFIs should make an informed assessment of the level of adequacy AML/CFT Control measures supported with statistical evidence were appropriate. Examples of the assessment of the risk mitigating measures are indicated in the **Table 4.**

Table 4: Examples of Ratings for Mitigation Measures

Risk Mitigation Factor	Weight (% Optional)	Average** Rating	Weighted Rating
Corporate Governance and role of Board	20	2	0.40
Compliance and Management Information	10	2	0.20
Audit and Compliance Function	25	1	0.25
AML/CFT Policies, Procedures and Controls	20	2	0.40
Suspicious Transaction Reporting	15	3	0.45
AML/CFT Resources, Staff and Training	10	2	0.20
Total Average	100	12.0	1.90

***Each Risk Mitigation factor may have several risk mitigation parameters as explained in this guideline and other guidelines like the CDD, STR and TFS guidelines issued by the Bank of Uganda, hence the need to obtain the "Average Rating".*

6. After assessing the elements of a mitigating measure, a (weighted) rating can be computed for that overall mitigating measure. Here, the application of weights is also optional, and the specific weights used in Table 4 are illustrative only, not prescriptive. For the assessment of mitigating measures, a more qualitative approach can also be used, as shown in Table 5.

Table 5: Qualitative Assessment of Mitigations measures

Indicator	1.Strong Controls	2.Moderate Controls	3. Needs Improvement Controls	4. Wea
Governance and Board	There is an active board, and senior management is involved in monitoring ML/TF/PF risk and approves and regularly updates the institution's ML/TF/PF risk appetite, risk analysis, and AML/CFT/CPF policies and procedures.	There is a reasonably active board, and senior management is involved in monitoring ML/TF/PF risk and approves and updates on an irregular basis the institution's ML/TF/PF risk appetite, risk analysis, and AML/CFT/CPF policies and procedures.	There is limited involvement of the board or senior managers in monitoring ML/TF/PF risk, and they are sometimes involved in updating the institution's ML/TF/PF risk analysis and significant AML/CFT/CPF policies and procedures.	There involve board manage monito ML/TF and th involve institut ML/TF analysi AML/C policies procedu
Compliance Function	The compliance function is independent, has sufficient and skilled resources to fulfil its role in a timely manner, and is managed by an experienced person.	The compliance function is independent, generally has adequate resources to fulfil its role, and is managed by an experienced person	The compliance function is not entirely independent, does not have appropriately skilled resources, and is not managed by an experienced person.	The functio indepe not ha resourc not ma suitabl experie individ
AML/CFT Policies and Procedures	The SFI has in place adequate and effective AML/CFT/CPF Polices and procedures for all risk areas and no non-compliance issues have been	The SFI has in place adequate and effective AML/CFT /CPF Policies and procedures for all risk areas and only minor shortcomings/ non-compliance	The SFI has adequate AML/CFT /CPF Policies and procedures for all or some risk areas and there are several shortcomings/	The ins signific deficie AML/C framew The adequa AML/C

	raised by Regulator or external reviews (External/Internal Audits).	issues identified or have been raised by Regulator or external reviews (External/Internal Audits).	non-compliance issues identified or have been raised by Regulator or external reviews (External/Internal Audits).	Policies procedu or som and signific shortco non-co issues have be Regulat externa (Extern Audits)
Suspicious Transaction Reporting	The SFI has in place an automated suspicious transaction monitoring system. There is a mechanism in place to investigate alerts and report suspicious transactions to the FIA and no non-compliance issues have been raised by Regulator or external reviews (External/Internal Audits).	The SFI has in place an automated suspicious transaction monitoring system. There is a mechanism in place to investigate alerts and report suspicious transactions to the FIA and only minor shortcomings/non-compliance issues have been raised by Regulator or external reviews (External/Internal Audits).	The SFI has in place an automated suspicious transaction monitoring system. There is a mechanism in place to investigate alerts and report suspicious transactions to the FIA and several shortcomings/non-compliance issues have been raised by Regulator or external reviews (External/Internal Audits).	The S place automa suspici transac monito There mechan place t alerts suspici transac FIA an shortco complia have be Regulat externa (Extern Audits)
AML/CFT/CPF Resources, Staff and Training	The SFI has resources and staffing dedicated to AML/CFT/CPF compliance. There is a training plan in place that is being implemented by the Compliance department and no non-	The SFI has resources and staffing dedicated to AML/CFT/CPF compliance. There is a training plan in place that is being implemented by the Compliance department and minor shortcomings/non-	The SFI has resources and staffing dedicated to AML/CFT/CPF compliance. There is a training plan in place that is being implemented by the Compliance department and several shortcomings/non-	The resourc staffing to AM complia is a trai place t implem the departr signific shortco

	compliance issues have been raised by Regulator or external reviews (External/Internal Audits).	compliance issues have been raised by Regulator or external reviews (External/Internal Audits).	compliance issues have been raised by Regulator or external reviews (External/Internal Audits).	compli have be Regula externa (Extern Audits)
Compliance and Management Information System	The SFI has in place a mechanism to generate detailed AML/CFT/CPF – specific management information system reports. These reports are made available and discussed at both management and board level and no non-compliance issues have been raised by Regulator or external reviews (External/Internal Audits).	The SFI has in place a mechanism to generate detailed AML/CFT/CPF – specific management information system reports. These reports are made available and discussed at both management and board level and minor shortcomings/non-compliance issues have been raised by Regulator or external reviews (External/Internal Audits).	The SFI has in place a mechanism to generate detailed AML/CFT/CPF – specific management information system reports. These reports are made available and discussed at both management and board level and several shortcomings/non-compliance issues have been raised by Regulator or external reviews (External/Internal Audits).	The S place a to gene AML/C specific manage informa reports reports availab discuss manage board signific shortco compli have be Regula externa (Extern Audits)

7. The Residual risk is the assessed risk after mitigation measures have been applied to the inherent risks. For example, an SFI with weak AML/CFT/CPF controls may not be high-risk if the inherent risks are low (although, over time, criminals may exploit the weaker controls, causing a change in the entity's inherent risk exposure). Similarly, an entity with high inherent risks may not necessarily be high-risk if strong AML/CFT/CPF controls are applied so that the residual risks are lower. Therefore, evaluating residual risks is an important component in establishing the risk profile of the SFI.

8. There are various options to estimating residual risk, but a correlation matrix approach is a practical option that can be estimated using the three-level risk-rating methodology described in Table 6. For the example provided in Table 6, where the weighted inherent risk rating is medium and the weighted rating of the mitigating measures is satisfactory, the residual rating assessment would be as follows: total weighted inherent risk rating: **medium;** total weighted mitigating measures rating: **strong** and residual risk: **medium**

Table 6 Example of a Matrix for Estimating Residual Risk

Inherent Risk Rating	Mitigating Measures Rating		
	Strong	Moderate	Weak
Low –(L)	L	L	M
Medium – (M)	L	M	M
High (H)	M	H	H

9. The residual risk assessment should not take a purely quantitative approach based solely on numerical risk scores. Where SFIs have significant concerns about the potential impact of ML/TF/PF risk the SFI should have the ability to reflect such concerns in the residual risk assessment. Additionally, no matter how robust AML/CFT/CPF controls are, inherent risks cannot be mitigated entirely. Therefore, the SFI will always have to manage the remaining residual risks in line with their risk appetite.

Table 7: Example of Risk Factors and sub risk factors Risk Assessment Model (for both entity and individual customer case)

Risk Category	Risk Sub-Category	Individual Risk
Environmental Risk	Predicate offence/Money Laundering	Corruption
		Tax Evasion (trade-based money laundering)
		Human Trafficking
		Dealing in Counterfeit
		Fraud Cybercrime
		Drug trafficking
		Illegal Mining
	Terrorist Financing/Target Financial Sanctions	High-risks customers and high-risks customer transactions
Customer Risk	Customer Type Risk	Legal Form (natural person, legal person or legal arrangement)
		E.g. proportion of PEPs, proportion of legal persons in high-risk business sectors, based on FIA typology or National risk assessment etc, proportion of Lawyers and Accountant, dealers in precious metal, accountant. **NB:** The assessment of induvial risk should at the minimum consider the emerging AML/CFT/CPF trends, National risk Assessment Reports,

		the banks own assessment of customer type risk amongst others/
	Customer footprint	Customer Location Risk
		Customer Business Risk
Delivery Channel Risk	Non-Face-to-Face Risk	Channel Non-face -to-face risk
	Third Party Use Risk	Channel third party use risk
		Channel third party location
Products and Services*		Product 1*
		Product 2*

* Note – the products and services relevant to the SFIs should be added and assessed individually at the time of the assessment so the number of products of products and services offered will determine the number of risk ratings in the product risk section.

1. Environmental Risk

a) Environmental risk considers the external and internal environments of the SFI. Predicate crimes that can give rise to ML/TF/PF are considered. The SFI's vulnerability to these crimes (as per the National Risk Assessment) is assessed. This vulnerability may be because the types of customers are likely to be involved in the commission of one or more predicate crimes and/or is seeking to use products and services to launder the proceeds of a predicate crime. Predicate crimes can be grouped into several categories at least depending on the National Risk Assessment findings.

b) The internal vulnerability of the SFI being used to launder money, finance terrorism, or breach targeted financial sanctions is also considered. The environmental inherent ML/TF/PF risks are assessed and rated by applying a combination of risk likelihood and risk impact, is indicated in Table 8:

Table 8: Assessment of Environmental inherent risk rating

Environmental Inherent Risk Rating				
Impact				
Likelihood		**Minor**	**Moderate**	**Major**
	Very Likely	Medium	High	High
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium

c) The likelihood and impact ratings when assessing inherent environmental ML/TF/PF risk are defined as follows:

Likelihood

Very Likely	Almost certain that the risk will occur several times based on it occurring more than once previously and being expected to occur more than once in the future.
Likely	High probability the risk will occur at least once based on it occurring previously and it being expected to occur again.
Unlikely	Low probability that the risk will occur based it having not occurred previously and not being expected to occur in the future.
Impact	
Major	The risk occurring could result in significant financial penalties (with reference to the size and profitability of the SFI) and/ or result in limitations or restrictions on business activities which could affect the SFI's ability to continue as a going concern.
Moderate	The risk occurring could result in financial penalties and/or limitations or restrictions on business activities but would not affect the SFI's ability to continue as a going concern.
Minor	The risk occurring may result in financial penalties, but these are unlikely to affect the SFI's ability to continue as a going concern.

d) Environmental residual risk Residual environmental ML/TF/PF risks are assessed by overlaying the inherent ML/TF risk with an assessment of the controls to mitigate that risk, using the matrix in **Table 9**.

Table 9: Assessment of Environmental Risk Residual Risk

Environmental Residual Risk Rating		**Control Assessment**		
		Strong	**Moderate**	**Weak**
Environmental Inherent Risk Rating	**High**	Moderate	Moderate	High
	Moderate	Low	Low	High
	Low	Low	Low	Medium

2. Customer Risk

a) The customer type risk considers the vulnerability that customers may be involved in ML/TF/PF activities. ML/TF/PF customer risk is significantly influenced by the nature and/or attributes of a customer. The Customer inherent risk at an SFI level is assessed through a combination of:

i. Customer type risk

This is a combination of the *nature of the customer (natural person, legal person or arrangement)* and *whether customers (form)* are politically exposed persons (PEPs), a non-government organisation, lawyers, accountants,

dealers in precious metals amongst other customers who may be considered requiring profiling by the SFI.

The form of the customer and the percentage of each customer (including individuals) that have been identified, through customer due diligence, to represent a higher ML/TF/PF risk contributes to rating the customer base as higher footprint ML/TF/PF risk. The greater the percentage (which should be set for each risk rating score) of customer for identified as high-risk, in the customer base, the higher the risk rating. For example, the higher the percentage of PEP's in the customer base, the higher the risk rating. Customer type risk is assessed using the matrix below for each customer nature versus customer form for all the customer type identified by the SFI. The illustration in **Table 10** as a case for a PEP customer:

Table 10: Assessment of Customer Type Inherent Risk

Customer Type		**Customer PEP Risk**		
		High	**Medium**	**Low**
Customer nature (natural or legal person or legal arrangement	**High**	High	High	Medium
	Medium	High	Medium	Medium
	Low	Medium	Medium	Low

ii. Customer footprint risk.

This is a combination of *customer location risk* and *business risk assessment*. The customer location risk relates to where customers are located, based, or have a contact address. Where customers are overseas or in a higher ML/TF/PF risk country it may contribute to rating the customer base as representing a higher footprint ML/TF/PF risk. The higher the percentage *(SFIs should establish plausible thresholds)* of overseas customers in the customer base the higher the percentage in countries rated as high-risk or restricted, the higher the customer location risk rating.

Customer business risk relates to ***nature of business*** activities that the customers undertake or are engaged in, as some activities are inherently more vulnerable than others to ML/TF/PF *(SFIs should identify and assess the nature of businesses that are high-risk).* Where customers are engaged in or are undertaking higher ML/TF/PF risk business activity, this may contribute to rating the customer base as higher footprint ML/TF/PF risk. The higher the percentage of customers in higher risk business activities, the higher the risk rating. Customer footprint risk is assessed using the matrix in **Table 11:**

Table 11: Assessment of customer footprint Inherent Risk

Customer Footprint Risk		**Customer Business Risk**		
		High	**Medium**	**Low**
	High	High	High	Medium

Customer Location Risk	**Medium**	High	Medium	Medium
	Low	Medium	Medium	Low

b) The overall inherent customer ML/TF/PF risk is assessed by applying a combination of customer footprint risk and customer type risk, using the Matrix in **Table 12:**

Table 12: Overall Inherent Customer ML/TF/PF Risk Assessment

Customer Inherent Risk Rating (IRR)		**Customer Type Risk**		
		High	**Medium**	**Low**
Customer Footprint Risk	**High**	High	High	Medium
	Medium	High	Medium	Medium
	Low	Medium	Medium	Low

c) Customer residual risk Residual customer ML/TF/PF risks, are assessed by overlaying the inherent ML/TF/PF risk with an assessment of the controls to mitigate that risk, using the following matrix in **Table 13:**

Table 13: Overall Customer ML/TF/PF Risk

Customer Inherent Risk Rating (IRR)		**Control Assessment**		
		Strong	**Moderate**	**Weak**
Customer Inherent Risk Rating	**High**	Medium	High	High
	Medium	Low	Low	Medium
	Low	Low	Low	Medium

3. Other Risk Factors

SFIs may develop a similar approach as demonstrated in the customer risk assessment for the delivery channels, and products and services.

a) ***Delivery Channels Risks***

i. The ML/TF/PF risk is significantly influenced by the nature and/or attributes of the channels used to deliver products and services to customers. Channel risk is determined by whether the delivery of a product or service involves face to face contact with the customer, as face to face contact limits the ability for customer anonymity and facilitates establishing whether the customer is who they are claiming to be. However, non face-to-face identification and transactions which are deemed high-risk could become a medium level of risk or even a low risk in the context of the prevention of ML/TF/PF when using reliable digital identities. The use of third parties as part of the delivery chain of a product or service also creates a higher ML/TF/PF channel risk.

ii. Delivery Channel inherent risk is assessed through a combination of non-face to face customer engagement risk and third-party risk. Non-face to face

risk assesses the extent to which customers are not met face to face. Where a customer is not met in person (face to face) there is an increased vulnerability that the customer may not be who they claim to be, which may contribute to rating the channels used by the SFI as representing a higher ML/TF/PF risk. The higher the percentage of customers that are not met face to face, the higher the non-face to face risk rating. Data on the methods used to engage customers or deliver products and services to customers is collected to provide context to the risk of the channels used.

iii. Third party risk is a combination of third-party use by the SFI to engage customers and third-party location risk assessments: ***Third party use*** risk assesses the use of third parties to engage and attach customers for their products and services. The level of use of third parties to engage customers may contribute to rating the channel as representing a higher ML/TF/PF risk. The higher the percentage of customers engaged through third parties, the higher the third-party use risk rating. *Third party location risk* assesses where third parties used by the SFI to engage customers are located, based, or operate from. Where third parties are in a higher ML/TF/PF risk country, branches or locations it may contribute to rating the channels used by the SFI as representing a higher ML/TF/PF risk. The higher the percentage of third parties overseas or in high-risk jurisdictions and the higher the percentage of third parties in countries, branches rated as high-risk or restricted, the higher the third-party location risk rating additional data that provides context to the channel include the details of third parties used to engage customers or that undertake business activities/operations that involve customer contact.

b) Product and Services Risk

i. The ML/TF/PF risk is significantly influenced by the nature and/or attributes of products and services. Product and service risk is determined by whether the attributes of a product or service offer features or characteristics that can be used to facilitate ML/TF/PF. The methodology applied to assess product ML/TF/PF risk is based on different attributes that are risk factors to whether the product or service is more vulnerable and therefore is higher risk.

ii. Inherent product or service ML/TF/PF risk is assessed by applying a combination of a flexibility rating and higher risk product classification. The flexibility of a product or service is an assessment of how much functionality and capability it allows the customer. The risk factors that make a product or service more vulnerable to ML/TF/PF risk are:

- Customer or user anonymity.
- The use or access by third parties.
- The availability or use overseas; and
- The ability to use or gain access to cash.

iii. Products or services that have been identified as representing a higher ML/TF/PF risk by typologies or case studies, are considered to represent a higher risk. Where the product or service has been determined to be higher risk, a risk flag is assigned, which increases the inherent risk rating derived from product/service flexibility rating. Additional data that provides context to the risk of the product or service include:

- The percentage of customers using the product or services.
- The amount of revenue the product or service generates.
- Whether the product or service is subject to monitoring; and
- The number of reports of suspicion made in the last 12 months involving the product or service.

c) Country Risk

Country risk is the assessment of a country's or jurisdiction's vulnerability to ML/TF/PF and Targeted Financial Sanctions (TFS). Country risk ratings are relevant to the location of business operations, customers, and third-party distributors. The following criteria may be used by SFIs to apply each country with their risk rating:

Ratings	Criteria
Restricted	Any country with person (s) or entities currently subject to TFS imposed by the United Nations Security Council Resolutions (listed on the FATF or FIA Website every Feb/march, June/July and October/November each year), and other countries in independent of the FATF Call. TFS include: • Freezing of assets, financial measures, restrictions on investments, or arms export involving financial assistance (EU) • Blocking of property, financial restrictions (US) • Any Other issues that the SFI may deemed sufficient to warrant restriction
HIGH	Any country that is currently subject to any other sanctions imposed by the UN, US, EU such as specific trade embargo's; or Any country that has historically been sanctioned by UNSCR; and appears on 2 or more of the following lists: • Listed by the FATF as having strategic AML/CFT/CPF deficiencies • Listed by the US State Department as being a State Sponsor of Terrorism or Terrorist Safe Haven • Listed on the Transparency International Corruption Perceptions Index with a score of 40 or less

	• Listed on the Financial Secrecy Index, issued by the Tax Justice Network, with a score of 60 or more • Any Other list that the SFI may deemed sufficient to warrant classifying as high-risks
MEDIUM	Any country that appears on only 1 of the following lists. • Listed by the FATF as having strategic AML/CFT/CPF deficiencies • Listed by the US State Department as being a State Sponsor of Terrorism or Terrorist Safe Haven • Listed on the Transparency International Corruption Perceptions Index with a score of 40 or less Listed on the Financial Secrecy Index, issued by the Tax Justice Network, with a score of 60 or more • Results of the Global Forum peer reviews • OECD peer reviews of the implementation of the OECD Anti-Bribery Convention • UNODC's reviews of the implementation of UNCAC • Any Other list of factors that the SFI may deemed sufficient to warrant classifying as medium risks
LOW	Any country that does not appear on any of the following lists, OR any country that is a FATF member but only appears on 1 of the following lists: • Listed by the FATF as having strategic AML/CFT/CPF deficiencies • Listed by the US State Department as being a State Sponsor of Terrorism or Terrorist Safe Haven • Listed on the Transparency International Corruption Perceptions Index with a score of 40 or less Listed on the Financial Secrecy Index, issued by the Tax Justice Network, with a score of 60 or more • Any Other list or factors that the SFI may deemed sufficient to warrant classifying as low risks

Annex 3: Hypothetical Example of the presentation of Risk Assessment Results/Report

Sections	Description
Executive Summary	Prepare brief on the SFI's consolidated view of all the ML/TF/PF risk. Mention whether the ML/TF/PF risk is considered as a material risk with justifications.
Explanation of Risk Categories	A consolidated view of the risk ratings for each of the following risk categories (if applicable): i. Environmental Risk ii. Customer Risk iii. Business Risk iv. Delivery Channel Risk

	v. Product and Services vi. Country risk Risk Included is a summary of the inherent risk ratings, controls, and residual risk rating for each risk category and their sub-categories.
Risk Sub-Categories	A consolidated view of the SFI's risk rating of each of the risk sub-categories that make up a risk category.
Individual Risk	A consolidated view of the SFI's risk rating of each risk component that make up a risk sub-category.
Risk Assessment	A detailed assessment of the risk, the risk's indicators, the inherent risk, the controls, the effectiveness of the controls and the residual risk rating for each risk assessed.

References:

1. *Anti-Money Laundering Act 2013 (as amended) and Anti – Laundering Regulations 2015*
2. *Basel Core Principles for Effective Supervision*
3. *FATF, Guidance for risk-based approach – The Banking Sector (October 2014)*
4. *FATF, Methodology for assessing technical compliance with FATF Recommendations and the effectiveness of AML/CFT Systems.*
5. *Financial Conduct Authority (FCA) published guidance to clarify expectations when significant AML weaknesses persist in small banks*
6. *World Bank, Preventing Money Laundering and Terrorist Financing; A Practical guide for bank supervisors: 2nd Edition.*