

MONEY LAUNDERING (ML)/TERRORIST FINANCING (TF)/PROLIFERATION FINANCING (PF) RISK ASSESSMENTS GUIDANCE NOTES

Issued: 1 June 2023

Revised: 29 October 2026

SUPERVISORY AND REGULATORY GUIDELINES: 2026
ML/TF/PF Risk Assessments Guidance Notes
Issued: 1 June 2023
Revised: 29 October 2026

TABLE OF CONTENTS

INTRODUCTION **3**
PURPOSE **3**
SCOPE **4**
APPLICABILITY **4**
DEFINITIONS **5**
RISK ASSESSMENT METHODOLOGY **7**
DETERMINING RISK APPETITE AND RISK TOLERANCE **8**
Risk Appetite 8
Risk Tolerance 8
IDENTIFY AND ASSESS INHERENT RISKS **9**
Customer Risk Factors 9
Country/Geographic Risk Factors 9
Products/Services Risk Factors 10
Delivery Channels Risk Factors 11
Other Qualitative and Emerging Risk Factors 12
ESTABLISH CONTROLS AND MEASURE EFFECTIVENESS **13**
EVALUATE RESIDUAL RISKS **14**
MONITOR AND REVIEW OF THE RISK ASSESSMENT **14**

INTRODUCTION

1. The Central Bank of The Bahamas ("the Central Bank") is responsible for the licensing, regulation and supervision of Supervised Financial Institutions ("SFIs") operating in and from within The Bahamas pursuant to the Banks and Trust Companies Regulation Act, 2020 ("the BTCRA"), The Bahamas Co-operative Credit Unions Act, 2015 ("the BCCUA"), Payment Systems Act, 2012 ("the PSA") the Payment Instruments (Oversight) Regulations, 2017 ("PIOR"), the Bahamian Dollar Digital Currency Regulations, 2021, and the Central Bank of The Bahamas Act, 2020 ("the CBA")

2. All SFIs are required to adhere to the Central Bank's licensing, regulatory, and prudential requirements, as well as ongoing supervisory programmes, including periodic onsite examinations and required regulatory reporting. SFIs are also expected to conduct their affairs in conformity with all other Bahamian legal requirements.

3. The Central Bank of The Bahamas ("the Central Bank") requires that all Supervised Financial Institutions ("SFIs") implement an appropriate Money Laundering/Terrorist Financing/Proliferation Financing (ML/TF/PF) Risk Assessment framework. These Guidance Notes serve as a general guide and set out the Central Bank's minimum expectations with regards to SFIs' ML/TF/PF Risk Assessment process.

PURPOSE

4. The purpose of the ML/TF/PF Risk Assessment is to promote improvements in financial crime risk management through identifying, assessing, and monitoring the risks faced by SFIs. The results of a risk assessment can be used for various purposes, including but not limited to the following:

    i. To identify gaps or opportunities for improvement in AML/CFT/CPF policies, procedures, and processes;
    ii. To make informed decisions about the SFI's risk appetite as well as the implementation of controls and the allocation of resources;
    iii. To assist management in understanding how the structure of a business unit or business line's AML/CFT/CPF compliance programme aligns with its risk profile;
    iv. To develop risk mitigation strategies including applicable internal controls and thereby lower a business unit's or business line's residual risk exposure;
    v. To ensure senior management is made aware of the key risks, control gaps and remediation efforts;
    vi. To assist senior management with strategic decisions in relation to commercial exits and disposals;
    vii. To assist management in ensuring that resources and priorities are aligned with its risks; and
    viii. To ensure regulators are made aware of the key risks, control gaps and remediation efforts across the SFI.

SCOPE

5. These Guidance Notes should be read in conjunction with Section II – Internal Controls, Policies and Procedures, particularly paragraphs 31–33 (Risk Self-Assessments and Risk Assessment Process), of the Central Bank's current *Guidelines for Supervised Financial Institutions on the Prevention of Money Laundering, Countering the Financing of Terrorism and Proliferation Financing*. Paragraphs 34–38 should also be considered, where relevant, in relation to new products, practices and technological developments.

6. These Guidance Notes outline the minimum elements to be considered by Supervised Financial Institutions (SFIs) when conducting their money laundering (**ML**), terrorist financing (**TF**) and proliferation financing (**PF**) risk assessments. They supplement the applicable requirements of the Central Bank's AML/CFT/CPF Guidelines and should be applied in conjunction with relevant Bahamian legislation and other applicable regulatory requirements.

APPLICABILITY

7. These Guidance Notes apply to SFIs incorporated in The Bahamas and are to be applied as appropriate to the nature, complexity and inherent ML/TF/PF risks in the SFIs' business activities. These Guidance, however, do not directly apply to nominee trust companies[1].

8. In applying these Guidance Notes, SFIs should have regard to the following regulatory and international guidance, as relevant to their licensed activities, business models and ML/TF/PF risk profiles:

   i. The Central Bank of The Bahamas' current Guidelines for Supervised Financial Institutions on the Prevention of Money Laundering, Countering the Financing of Terrorism and Proliferation Financing, together with other applicable Central Bank guidance, notices and directives.
   ii. The Financial Action Task Force (FATF) Risk-Based Approach Guidance for the Banking Sector.
   iii. The FATF Guidance for a Risk-Based Approach for Money or Value Transfer Services.
   iv. The FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers, where relevant to the institution's activities and applicable supervisory framework.
   v. The FATF Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, where relevant to the products, services and delivery channels offered.
   vi. The applicable FATF Recommendations, interpretive notes and other relevant FATF guidance addressing risk assessment, risk mitigation and the identification and assessment of ML/TF/PF risks.

[1] While nominee trust companies are exempt from these Guidance Notes, it is the Central Bank's expectation that the risk assessments of their parent companies will include their ML/TF/PF risks.

9. The above sources should be considered alongside applicable Bahamian legislation and regulatory requirements. SFIs should take account of relevant amendments to the FATF Recommendations and updates to the cited guidance, having regard to the current versions available. The inclusion of the above external guidance does not replace any applicable legal or regulatory obligation.

DEFINITIONS

10. For the purpose of these Guidance Notes the following acronyms or terms will be used:

"**AML**" means anti-money laundering;

"**CFT"** means countering financing of terrorism;

"CPF" means countering proliferation financing;

"corrective action plan" means a time-specific collection of remediation steps designed to correct possible and existing deficiency gaps;

"customer[2]" means any of the following –

a) a person for whom a transaction or account is arranged, opened or undertaken;
b) a signatory to a transaction or account;
c) a person to whom an account or rights or obligations under a transaction have been assigned or transferred;
d) a person who is authorised to conduct a transaction or control an account;
e) a person who attempts to take any of the actions referred to in (a) to (d) above; or
f) such other person as may be prescribed by the Minister[3];

"identified risk"[4] means corruption, cybercrime, human trafficking, money laundering, or financing of proliferation of weapons of mass destruction, terrorism or financing of terrorism, or such other risk as the Minister may prescribe by regulations;

"impact" means the adverse effect that may follow due to a risk event occurring;

"inherent risk" means the risk associated with any current or future process or activity before the implementation of risk mitigating mechanisms and controls;

"inherent vulnerability variable'' relates to specific features of a particular risk factor. As an example, a client base profile may vary from product to product and consequently affect its vulnerability to ML/TF/PF risk;

"internal controls" means a process, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance;

"likelihood" means the probability of a risk event occurring;

[2] FTRA, 2018
[3] Refers to the Minister of Finance
[4] FTRA, 2018

"**money laundering**"[5] means —

a) any offence referred to in Part III of the Proceeds of Crime Act, 2018 ("POCA, 2018");
b) any act or words which constitutes an attempt, conspiracy, or incitement to commit an offence referenced in paragraph (a);
c) any act or words which constitutes aiding, abetting, counselling or procuring the commission of an offence referenced in paragraph (a); or
d) conduct committed outside The Bahamas which would constitute an offence specified in paragraph (a), (b) or (c) if the conduct was committed in The Bahamas;

"**politically exposed person"**[6] means an individual who is or has been entrusted—

a) with a domestic prominent public function, inclusive of a head of state or government, legislator, politician, senior government, judicial or military official, senior executive of a state-owned corporation, or important political party official;
b) with a prominent public function by a foreign jurisdiction, inclusive of, a head of state or government, legislator, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation, or senior political party official; or
c) with a senior position at an international organisation or branch thereof, domestic or foreign, and includes a family member or close associate of a politically exposed person;

"proliferation financing"[7] refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations;

"residual risk" means the risk that remains after controls are applied to the inherent risk;

"risk" means the possibility that an event of a given impact will occur, adversely affecting the achievement of objectives;

"risk appetite" means the aggregate level and types of risk a SFI is willing to assume to achieve its strategic objectives and business plans;

"risk appetite statement" means the written form of the aggregate level and types of risk that a SFI is willing to accept, or to avoid, in order to achieve its business objectives;

"risk assessment" means the combined effort of identifying and analysing potential events that may negatively impact individuals, assets, and/or the environment;

[5] POCA, 2018
[6] FTRA, 2018
[7] GFSR Guidance Note on Proliferation and Proliferation Financing, 2026

"risk owner(s)" means the first line decision maker(s) with the accountability, authority and responsibility to manage risks within their span of control;

"risk profile" means a composite view of the risk assumed at a particular level of the SFI, or aspect of the business, that positions management to consider the types, severity and interdependencies of risks and how they may affect performance relative to the strategy and objectives;

"risk tolerance" is the variation around the prescribed risk appetite that the SFI is willing to take;

"risk triggers" means the risk symptoms, warning signs or indicators of an event or condition that breaches the risk tolerance has occurred;

"terrorist"[8] includes a person who —

a) commits a terrorist act by any means directly or indirectly, unlawfully and wilfully;
b) participates as an accomplice in terrorist acts or the financing of terrorism;
c) organises or directs others to commit terrorist acts or the financing of terrorism; or
d) contributes to the commission of terrorist acts or the financing of terrorism by an individual or a group of persons acting with a common purpose where the contribution is made intentionally —
   i. with the aim of furthering the terrorist act or the financing of terrorism; or
   ii. with the knowledge of the intention of the individual or group of persons to commit the terrorist act or the financing of terrorism;

"terrorist financing"[9] involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organisations;

RISK ASSESSMENT METHODOLOGY

11. A SFI's risk-based approach should be built on their risk assessment methodology. The processes for identifying and evaluating risk variables, scoring criteria, and weights should be contained in the SFI's internal policies and procedures documentation. It should also give internal stakeholders a blueprint for a replicable procedure to improve upon and allow third parties to test the design and operational effectiveness of the risk assessment. Moreover, risk owners should be clearly identified.

12. The risk assessment should be based on a SFIs' business model and should be logical, comprehensive, and relevant to ensure the timely identification, management and escalation of breaches in material risk limits/tolerance levels.

13. SFIs should take into account the threats and vulnerabilities that have been identified in The Bahamas' National Risk Assessment. SFIs should assess how these (and any other aspects of their business) make their business vulnerable to identified risks. SFIs should assess the probability or likelihood that these aspects of their business could result in ML/TF/PF risks. The end-result of this step will be a likelihood rating for each

[8] Anti-Terrorist Act (ATA, 2018)
[9] IMF AML/CFT-Topics

of the risk areas of your business. For example, a SFI may rate each area from a range of high (highly likely) to low (unlikely) to be used for ML/TF/PF risks.

14. SFIs should employ a three lines of defence regime to ensure effective risk and control measures. These are as follows:

    i. First line roles deliver products/services to clients while managing risk (e.g. front office, customer-facing activity);
    ii. Second line roles deliver expertise, support, monitoring, and challenge on risk-related matters (e.g. risk management/compliance function); and
    iii. Third line roles deliver independent and objective assurance and advice on all related matters (e.g., internal audit).

15. It is important to note that the size and complexity of the SFI will determine the characteristics of each line of defence.

16. SFIs should also establish robust ML/TF/PF risk management policies and procedures, and conduct periodic risk assessments that are reviewed and approved by the Board and senior management and submitted to the Central Bank.

17. Although SFIs are not required to follow a prescribed risk assessment methodology, the following sections lay out the main tenets that should be included within an effective ML/TF/PF risk assessment.

DETERMINING RISK APPETITE AND RISK TOLERANCE

Risk Appetite

18. SFIs are expected to determine their risk appetite, approved by the Board, and provide a risk appetite statement in the risk management policy and procedures documentation. Risk appetites may differ among SFIs depending on their sector, culture, and business objectives and may change over time.

Risk Tolerance

19. After establishing the risk appetite, SFIs should clearly document the deviations that are acceptable as well as where approving authority lies for exceeding risk appetite thresholds (i.e. an entity's risk tolerance). While risk appetite is often broad, risk tolerance is tactical, quantitative, and focused. It applies to significant objectives and cascades throughout the entity, providing guidance on a daily basis. There should also be a clear policy for the swift reporting and management of threshold breaches. By identifying the specific risk triggers for each event, SFIs can better oversee their risk management process.

20. In setting risk tolerance, SFIs should consider the relative importance of each objective. Highly significant objectives are often assigned low-risk tolerances. Optimising resource allocation becomes a specific consideration when deciding where to set tolerance. The lower the range of risk tolerance, the more likely it will be that greater resources are required to stay within that range.

IDENTIFY AND ASSESS INHERENT RISKS

21. Inherent risk factors should be categorised by customer, country/geographic area, products/services, transactions, delivery channels or other qualitative and emerging risks. SFIs should consider each risk factor individually and in combination with other risk variables to determine potential ML/TF/PF risks.

Customer Risk Factors

22. Determining the identity of a customer and the type of activity involved is a critical part of countering financial crime. SFIs must ensure that inherent risks are accounted for based on the composition of their customer base, exposure to high-risk legal entities or arrangements, and the complexity of those entities. Given the nature of ML/TF/PF risks, a SFI is severely exposed if it fails to identify the risks that are inherent in its customer base. Essentially, know your customer ("KYC") principles serve as the foundation of an effective risk management system. SFIs' risk management systems must account for atypical behavioural changes to ensure the timely detection of illicit transactions.

23. Notwithstanding the customer due diligence (''CDD'') and transaction monitoring activities that occur throughout the duration of the customer relationship, SFIs should segment their customers in order to identify patterns and trends. For example, customers should be identifiable based on whether they are legal or natural persons; low, medium, or high-risk; or where the customer is a PEP.

24. When identifying and assessing the risk associated with customers, including the beneficial owners of those customers, SFIs must consider all of the following risk factors, either individually or in combination:

    i. Whether a customer can issue bearer shares or has nominee shareholders;
    ii. Whether a customer engages in high levels of cash transactions or cash-equivalent intensive business;
    iii. Whether a customer is a PEP, family member or close associate of a PEP, and/or where the beneficial owner is a PEP;
    iv. Whether a customer is the subject of a law enforcement conviction or sanction;
    v. Whether a customer engages in business activities in a high-risk jurisdiction, or a jurisdiction known for corruption, terrorist activities, organised crime or drug production/distribution;
    vi. Whether a customer has corporate vehicle structures that have no clear commercial or economic rationale and/or lack transparency to identify beneficial owners;
    vii. Whether a customer is employed in a high risk industry; and
    viii. Whether a customer appears unable or reluctant to disclose details about the payee or beneficiary of a wire transfer or other information (e.g. address, contact information, etc.).

Country/Geographic Risk Factors

25. SFIs should consider the geographical region where their customers conduct business activities including multiple components such as: cross-border transactions, the

domicile or nationality of customers/beneficial owners, the geographical region in which the customer conducts business, including proximity to high-risk and sanctioned countries.

26. When identifying country/geographic risks, SFIs should evaluate ML/TF/PF risks associated with doing business, opening and servicing accounts, offering products and services and/or facilitating transactions involving certain geographic regions.

27. When assigning risk ratings to a country/geographic region that may pose ML/TF/PF risks, SFIs must consider:

    i. whether the country has been identified by reliable and credible sources (such as the FATF, CFATF or other FATF-Style Regional Bodies) as lacking appropriate AML/CFT/CPF laws, policies and compliance measures and where special attention should be given to business relationships and transactions;
    ii. whether the country has significant levels of organised crime, corruption, or other criminal activity, including being a source or transit country for illegal drugs, arms dealing, human trafficking, people smuggling and illegal gambling;
    iii. whether the country or geographic region is subject to sanctions, embargos imposed by the United Nations Securities Council or has had other similar measures imposed;
    iv. whether the country/geographic region is known for terrorist activities, or has terrorist organisations domiciled in the region; and
    v. whether the customer business relationship and/or associate doing business within a country/geographic region is known for high levels of ML/TF/PF risk.

Products/Services Risk Factors

28. Certain products and services are inherently more vulnerable to ML/TF/PF risks. SFIs' overall risk assessments should identify and assess all products (e.g. deposit accounts), and services (e.g. asset management) particularly those that have a high vulnerability to ML/TF/PF. Assessing the inherent vulnerability variable of each existing product and service contributes to a comprehensive risk assessment.

29. Based on the SFI's business model, the following products and services may be included (although not be limited to these) in the assessment: private banking, retail deposits, and deposits of legal persons, credit products for retail customers, small and medium-size businesses, large businesses, electronic banking, trade finance, digital assets, and wire transfers.

30. When assigning a risk rating to products and services, SFIs should consider:
    i. the nature, value, and complexity of the business (including the total size/volume and average transaction size);
    ii. the cross-border nature of transactions;
    iii. whether non-face-to-face customer acceptance and/or occasional transactions are conducted;
    iv. payments received from unknown or unrelated third parties;
    v. products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or money order; and

vi. the level of transparency of the products and/or services, the anonymity or layers of opacity of the customer, beneficial ownership, or those products or services that can readily transcend international borders, such as cash, online payment systems, stored value cards, money orders, mobile payments, prepaid cards and international wire transfers;
vii. use of new technologies or payment methods; and
viii. products or services that provide limited and defined services to certain types of customers to increase access for financial inclusion.

Sector-specific considerations

31. ML/TF/PF risks associated with the nature of their licensed activities, business models, customer bases, products and services. Relevant considerations may include, but are not limited to, the following:

i. **Banks:** Correspondent banking, trade finance, cross-border payments, private banking and other services involving complex transactions or higher-risk customers.

ii. **Co-operative credit unions:** Member savings and lending activities, cash-intensive transactions, transfers between members, and transactions inconsistent with a member's known profile or expected activity.

iii. **Money transmission businesses (MTBs):** Domestic and international remittances, higher-risk transaction corridors, agent networks, cash-based transfers, transaction volumes and frequency, and transfers involving third parties.

iv. **Trust companies:** The nature and complexity of fiduciary arrangements, trust structures, settlors, trustees, protectors and beneficiaries, and the transparency of ownership and control arrangements.

v. **Trust and company service providers (TCSPs):** Company formation and administration, nominee shareholder or director arrangements, complex corporate structures, beneficial ownership transparency and the use of legal persons or arrangements across multiple jurisdictions.

vi. **Payment service providers and electronic money activities, where applicable:** Digital payment channels, merchant relationships, stored-value products, prepaid payment instruments, transaction velocity, cross-border payment flows and reliance on agents or third-party service providers.

32. SFIs should determine the relevance and significance of these factors based on their individual risk profiles and document how identified risks are reflected in their risk assessment methodology, risk ratings and, where necessary, mitigating controls. These considerations should be read alongside applicable Central Bank requirements and relevant FATF sector-specific guidance.

Delivery Channels Risk Factors

33. When assessing delivery channel risk factors, SFIs should assess whether, and to what extent, the methods used to establish and maintain customer relationships, deliver products and services, and conduct transactions could increase inherent delivery channel risks.

34. SFIs should document and assign, where applicable, differentiated rating scales and weightings to delivery channel risks. The business unit or business line should determine the proportion of accounts or customers within each risk classification (e.g., *low, moderate, high or higher risk*) to determine the overall inherent delivery channel risk.

35. SFIs should consider the following inherent vulnerability factors that may indicate a higher risk when completing their risk assessments:

    i. Outsourced service arrangements involving intermediaries or introducers (for example, mortgage and deposit agents and brokers) that may not be subject to equivalent compliance laws and measures as the SFI, or may not be adequately supervised;
    ii. Use of electronic banking, telephone, mail and email correspondence as a substitute for face-to-face interaction with the customer;
    iii. Wire transfers payable upon presentation of client identification;
    iv. Use of digital onboarding processes and electronic identity verification, including circumstances where the reliability of identity verification may be difficult to establish;
    v. Use of agents, intermediaries or third-party service providers to onboard customers, initiate transactions or deliver financial services, particularly where oversight, monitoring or access to customer information may be limited;
    vi. Delivery channels that facilitate rapid, high-volume, anonymous or cross-border transactions, including mobile and internet-based payment services, where these characteristics increase the institution's exposure to ML/TF/PF risks;
    vii. Delivery channels that may facilitate the concealment of customer identity, impersonation, the use of false or stolen identity information, or activity inconsistent with the customer's known profile; and
    viii. The introduction of new delivery channels, significant changes to existing channels, or changes in the use of agents, technology or third-party service providers that may alter the institution's ML/TF/PF risk exposure.

36. SFIs should assess these factors in the context of their business models, customer profiles, products and services. The assessment should consider the effectiveness of controls applied to each delivery channel and the extent to which any remaining risks affect the institution's overall ML/TF/PF risk rating.

Other Qualitative and Emerging Risk Factors

37. SFIs should consider other qualitative risk factors and emerging risks that could have an impact on operational risks and contribute to an increased or decreased likelihood of ML/TF/PF. Qualitative risk factors such as significant strategy and operational changes could directly or indirectly increase inherent risks. These changes may require a review of existing, or the establishment of new internal controls.

38. Other vulnerable risk factors may include, but not be limited to, the following:

    i. Environmental and climate change risk;
    ii. IT system integration;

iii. Frequency of AML Compliance employee turnover;
iv. Material changes in business strategy and operational procedures not being assessed;
v. The existence (or lack thereof) of an independent compliance function;
vi. Impact of products and services on operations;
vii. The level at which SFIs rely on or change third party service providers;
viii. Introductions of new products and/or services;
ix. Acquisitions and/or mergers of business;
x. Projects and initiatives related to AML Compliance matters (e.g., remediation, elimination of backlogs); and
xi. Prior internal audit or regulatory remedial findings/enforcement actions.

ESTABLISH CONTROLS AND MEASURE EFFECTIVENESS

39. When establishing controls, SFIs must ensure that there is a clear connection between the inherent risks that were initially identified and the AML/CFT/CPF controls and measures. In other words, there should be a logical '*cause and effect'* relationship between the inherent risks and the controls that are implemented to mitigate these risks.

40. Furthermore, the ML/TF/PF risk assessments should include an evaluation of the effectiveness of a SFI's controls and an indication of any potential gaps or weaknesses within their risk management information system. SFIs should promptly adjust controls to reduce the ML/TF/PF risk posed by their business operations, customers, and external risk factors. SFIs should ensure that their programmes, policies and activities are designed and implemented to protect against the materialisation of ML/TF/PF risks.

41. SFIs are expected to test their controls based on their effectiveness in mitigating inherent risks. Control effectiveness should reflect the likelihood of control failure. For example, a control with a high likelihood of failure should not be acceptable for a high residual risk area.

42. AML/CFT/CPF controls are usually assessed across the following control categories:

i. Corporate Governance (See Corporate Governance Guidelines). For example, the process of reporting and escalating matters to Senior Management and Board;
ii. Know Your Customer Policies and Procedures;
iii. AML/CFT/CPF tiered training for staff, executive management, and the Board;
iv. Previous other risk assessments (onsite examinations, and AML/enterprise-wide assessments);
v. Operational Policies and Procedures;
vi. Record-Keeping and Retention;
vii. Effectiveness and independence of a Designated AML Compliance Officer/Unit; Compliance Function (i.e., Unfettered access to the Board or Board committee);
viii. Detection and unusual/suspicious transaction reports filing (i.e., ongoing transaction monitoring to account purpose and parameters);
ix. Sanctions screening and anti-terrorist financing risk measures; and

x. Targeted financial sanctions related to CFT or CPF controls.

EVALUATE RESIDUAL RISKS

43. After SFIs have identified and assessed their inherent risks and have established effective controls and measures to mitigate these risks, they must evaluate their residual risks. Residual risks are determined by balancing the level of inherent risks with the overall strength of the risk management controls. Residual risks are used to assess whether the ML/TF/PF risks within the SFI are being adequately managed. A high level of residual risk may suggest that additional controls should be implemented.

44. Regarding ML/TF risk management, SFIs will usually have the following three types of residual risk responses:
    i. **Avoid**: Discontinue performing the processes or activities that create the risk;
    ii. **Mitigate**: Add controls or strengthen existing controls; and
    iii. **Accept**: Adjust risk tolerance to incorporate the risk.

45. SFIs that decide to accept residual risks that are outside of their risk appetites should ensure that this is documented and approved by the Board. Residual risk acceptance should also be based on a thorough and transparent review process to ensure that the risks are appropriately estimated.

46. To evaluate residual risks, SFIs should develop and implement a risk rating scale that is appropriate to the nature, size, and complexity of their operations. It is possible to apply a three tier rating scale, to evaluate the residual risk on a scale of High, Moderate and Low. An alternative rating scale could also be used, for example a 5 point scale of Low, Low to Moderate, Moderate, Moderate to High, and High.

MONITOR AND REVIEW OF THE RISK ASSESSMENT

47. As mentioned in the AML/CFT/CPF Guidelines, risk assessments should be kept up-to-date through periodic reviews and when risk factors change. These risk assessments must be made available to the Central Bank **annually,** or as otherwise advised by the Central Bank. SFIs are also required to monitor compliance with internal policies, procedures, and controls, and enhance them if necessary. Where appropriate, having regard to the size and nature of their business, SFIs must engage an audit function to test the internal AML/CFT/CPF policies, controls and procedures.

48. A SFI's monitoring system should be adequate with respect to its size, its activities and complexity as well as the risks present within the institution. Where deficiencies are discovered that have not been resolved, such as an inadequate information technology monitoring system, a SFI should document its decision and be able to demonstrate to the Central Bank or third parties that it has in place an effective alternative. Monitoring systems should cover all accounts of the SFI's customers and transactions for the benefit of, or by the order of, those customers. As stated earlier, by risk rating the customers effectively, SFIs are better positioned to allocate resources to the higher risk areas.

49. For a ML/TF/PF risk assessment to be effective over time, SFIs must be able to demonstrate whether any risk factors have changed, internally or externally, and show whether any of the internal compliance policies, procedures, and controls have been updated. SFIs should undertake trend analysis of transaction activity to identify unusual business relationships and transactions in order to mitigate ML/TF/PF risks.

50. SFIs are encouraged to engage in periodic reviews, guided by their corrective action plans. SFIs are expected to test their controls to determine whether they are relevant and operating effectively. Controls should be tested periodically, based on the entity's risk appetite, tolerance, control frequency, and control effectiveness. SFIs should also determine the likelihood of control failure.

51. A SFI must conduct ongoing monitoring of its business relationships on a risk-sensitive basis. Ongoing monitoring means scrutinising transactions to ensure that they are consistent with what the SFI knows about the customer, and taking steps to ensure that the firm's knowledge of the business relationship remains current. As part of this monitoring, SFIs must keep documents, data and information obtained in the CDD process (including information about the purpose and intended nature of the business relationship) up to date. It must apply CDD measures where it doubts the veracity or adequacy of previously obtained documents, data or information. Furthermore, SFIs have a legal requirement to investigate unusual activity and to report suspicious activity to the Financial Intelligence Unit.