CENTRAL BANK of BELIZE

MONEY LAUNDERING/ TERRORIST FINANCING/ PROLIFERATION FINANCING RISK ASSESSMENT GUIDANCE NOTES FOR CENTRAL BANK-REGULATED INSTITUTIONS

CENTRAL BANK OF BELIZE
GABOUREL LANE
BELIZE CITY
BELIZE

MONEY LAUNDERING/ TERRORIST FINANCING/ PROLIFERATION FINANCING RISK ASSESSMENT GUIDANCE NOTES FOR CENTRAL BANK-REGULATED INSTITUTIONS

DECEMBER 2023

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AML/CFT/CPF	-	Anti-Money Laundering/Combating the Financing of Terrorism and Combating Proliferation Financing
CDD	-	Customer Due Diligence
Central Bank	-	Central Bank of Belize
FATF	-	Financial Action Task Force
KYC	-	Know Your Customer
ML/TF/PF	-	Money Laundering, Terrorist Financing and Proliferation Financing
MLTPA	-	Money Laundering and Terrorism (Prevention) Act
PEP	-	Politically Exposed Person

INTRODUCTION

1. The Central Bank of Belize (the Central Bank) requires that all Central Bank Regulated Institutions to 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 the ML/TF/PF Risk Assessment process.

2. Nothing herein prevents or limits the Central Bank from taking any course of action, it deems necessary, for the protection and strengthening of the financial system in Belize.

APPLICABILITY

3. These Guidance Notes apply to Central Bank Regulated Institutions and are to be applied as appropriate to the nature, complexity, and inherent ML/TF/PF risks in the institutions' business activities.

SCOPE

4. These Guidance Notes outline the elements that must be captured when institutions complete a ML/TF/PF risk assessment. It is intended to supplement the Central Bank's Anti-Money Laundering, Combating the Financing of Terrorism and Counter-Proliferation Financing Guidelines (AML/CFT/CPF Guidelines), and incorporates international best practices.

IMPLEMENTING A RISK-BASED APPROACH

5. The Central Bank recognizes the diversity of the institutions it regulates, and seeks to establish that, overall, processes appropriate to institutions are in place and are operating effectively.

6. Financial institutions are responsible to utilize the risk-based approach in meeting their AML/CFT/CPF obligations that are governed primarily by section 15 of the MLTPA.

7. Financial institutions must employ a risk-based approach in determining:

i. Appropriate levels of CDD measures, including whether to apply enhanced CDD;

ii. Mitigation measures commensurate with the risks posed by the financial institution's customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, products, services, transactions and delivery channels;

iii. The scope and frequency of ongoing monitoring;

iv. Measures for detecting and reporting suspicious transactions; and

v. Whether and how to launch new products, services, or technologies.

8. Financial institutions should document a risk-based approach AML/CFT compliance program. This approach requires an assessment of the ML/TF risks posed by the nature of the FI's business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme.

9. Senior Management must take ownership of, and responsibility for, the periodic evaluation to assess if and to what extent the financial institution is vulnerable to ML/TF/PF because of its activities and operations.

10. Senior Management must conduct a risk assessment in which it identifies and assesses the ML/TF risks and other integrity risks, considering risk factors including those relating to, at a minimum, the customers, countries and/or geographic areas, products, services, transactions, and delivery channels.

11. In the risk assessment Senior Management must consider the extent of the financial institution's exposure to risks by reference to its organizational structure, its corporate culture, its customers, the jurisdictions with which its customers are connected, its products and services, and how it delivers those products and services.

12. The risk assessment should be proportionate and tailored to the nature, size, and complexity of the financial institution's business. For example, large financial institutions are likely to have a more sophisticated system and methodology for conducting a risk assessment.

13. Some smaller financial institutions with limited range of customers and minimal products or services may be satisfied, on reasonable grounds, that standardized profiles for combinations of customers and services are appropriate. A focus of such financial institutions' efforts should be on those combinations of customers and services that fall outside any of the standardized profiles.

14. Regardless of its nature, size, and complexity, each financial institution must begin assessing the risks it faces either before commencing business or as soon as is reasonably practicable afterwards, ensuring that any ML/TF risks that may arise are effectively managed.

15. The risk assessment must be documented and kept up-to-date. This means a periodic and documented update of the risk assessment must be conducted, typically every one to three years, at a minimum, and/or following a 'trigger' event such as a serious compliance incident that has taken place, or major change of the financial institution's operations. The update must be approved by Senior Management and the risk assessment report should be made available, without delay, to the Central Bank upon request.

16. Following the risk assessment, Senior Management must also establish a documented AML/CFT/CPF strategy in accordance with its risk assessment. In the case where a financial institution forms part of a group operating outside Belize, that strategy must protect both its global reputation and its Belize business. Hence, an automatic adoption by the financial institution of the

global and/or regional risk assessment is unacceptable. Explicit attention should always be given to the specifics of Belize and the Belizean operations of the financial institution.

17. Additionally, each financial institution should ensure that it has sufficient capacity and expertise to manage the risks it faces. As risks and understanding of risks evolve, a financial institution's capacity, mitigating controls and expertise should also evolve proportionally.

A. Risk Management

18. Risk management is the process of measuring risks and applying appropriate mitigating measures to minimize risks. Senior Management of most financial institutions have experience managing the financial institution's inherent business risk and the effectiveness of controls to manage those risks. In the context of AML/CFT/CPF compliance, risk management is a tool to assist Senior Management in making decisions about the need for and allocation of AML/CFT/CPF compliance resources.

B. Conducting an Institutional Risk Assessment

19. Financial institutions should consider using the following steps to assess the level of identified risks that the business may face:

i. Identify and assess the institution's inherent risks. This is an assessment of the risk that the financial institution is currently undertaking.

ii. Establish risk-tolerance levels and compare with results in activity 19(i) above.

iii. Establish risk-mitigation measures by employing proper controls.

iv. Evaluate residual risks by determining the level of risk remaining after incorporating mitigation measures.

v. Monitor and review risks by using a proper governance regime.

20. Risk can be defined as a combination of the following:

i. The threat of an event;

ii. Vulnerability to such an event; and

iii. The consequences of the threatened event taking place.

21. A threat is a person, object, or activity with the potential to cause harm. In the AML/CFT/CPF context, a threat is the demand for services by criminals, terrorists, and their facilitators. Such demand is influenced by the types and scale of domestic and foreign crimes that result in tainted property. The national risk assessment process identifies threats at the national level. Financial institutions should use the national threats identified, as well as independently assess the threat of customers

attempting ML/TF at the business or transactional level. Customers who pose a greater threat of ML/TF are higher-risk customers.

22. A vulnerability is anything that may be exploited by a threat, or that may support or facilitate a threat's activities. A financial institution's AML/CFT/CPF context includes its vulnerabilities, products, services, transactions, and delivery channels and weaknesses in its AML compliance program.

23. A financial institution should consider consequences of an AML/CFT/CPF compliance failure including:

i. Legal consequences;

ii. Regulatory consequences;

iii. Financial consequences;

iv. Operational consequences; and

v. Reputational consequences.

24. In simple terms, risk is a combination of the likelihood that something might occur and the consequences of such an occurrence.

25. The process outlined below is a guide to assist financial institutions in assessing their level of identified risks.

I. Identify and Assess Inherent Risk

26. Inherent risk is the risk that naturally exists based on the business activity before there are mitigating controls in place. Financial institutions should consider all relevant information when identifying and assessing inherent risk. This includes considering how the various aspects of their business may be targeted as a viable option to facilitate money laundering, financing terrorism and proliferation.

27. At a minimum, this analysis must identify and assess the financial institution's inherent risks based on the following criteria:

i. The type of customers:

a. Target market segments;

b. Profile and number of customers identified as higher risk;

c. Complexity, volume, and size of customers' transfers, considering the usual activity and the risk profile of its customers (e.g., whether the ownership structure is highly complex; whether the customer is a politically exposed person (PEP); whether the customer's employment income supports account activity).

ii. The countries or jurisdictions its customers are from (or located), and where the financial institution has operations;

a. The AML/CFT/CPF laws, regulations and standards of the country or jurisdiction and quality and effectiveness of implementation of the AML/CFT/CPF regime;

b. Contextual factors such as political stability, maturity and sophistication of the regulator and supervisory regime, level of corruption, and degree of financial inclusion.

iii. The financial institution's products, services, transactions, and delivery channels:

a. Nature, scale, diversity and complexity of the financial institution's business activities including its geographical diversity;

b. Nature of products and services offered by the financial institution;

c. Delivery channels, including the extent to which there is direct interaction between the financial institutions and the customer or the extent to which reliance is placed on technology, intermediaries, third parties, correspondents or non-face-to-face access;

d. The degree to which the operations are outsourced to other entities in the Group or third parties; and

e. The development of new products and new business practices, including new delivery mechanisms and partners; or the use of new or developing technologies for both new and pre-existing products.

28. The financial institution should also consider variables such as the purpose of the business relationship, the level of customer assets, volume of transactions and the regularity or duration of the business relationship. Further, financial institutions should consider the threats and vulnerabilities that have been identified through any national risk assessment. Financial institutions should assess how these (and any other aspects of their business) make their business vulnerable to identified risks.

29. In addition to information from a national risk assessment, financial institutions should consider information obtained from relevant internal or external sources when conducting or updating risk assessments. These sources include, but are not limited to:

i. The financial institution's head of business lines and relationship managers;

ii. Internal/external audit and regulatory findings;

iii. Independent reviews;

iv. Sectoral emerging risks and typologies;

v. Corruption indices and country risk reports;

vi. Guidance issued by regulators;

vii. Threat reports and typologies issued by the FIU and law enforcement agencies;

viii. Independent and public assessment of a country's or jurisdiction's overall AML/CFT/CPF regime such as Mutual Evaluation Reports, IMF Financial Sector Assessment Programme Reports or Reports on the Observance of Standards and Codes; and

ix. Public sources of adverse news or relevant public criticism of a country or jurisdiction, including FATF, CFATF and other FSRBs public statements.

30. Financial institutions should then assess the probability or likelihood that the aspects of their business may result in ML/TF. The result of this step will be a likelihood rating for each of the risk areas of its business. For example, a financial institution may rate each area from a range of high (highly likely) to low (unlikely) to be used for ML/TF.

II. Establish Risk Tolerance

31. Risk tolerance is the level of risk that a financial institution is willing to accept, and impacts decision about risk mitigation measures.

32. Each financial institution should consider:

i. The risks it is willing and unwilling to accept;

ii. Risks that should be escalated to Senior Management for a decision; and

iii. Whether the financial institution has sufficient capacity and expertise to effectively manage the risks it has or is willing to accept.

III. Establish Risk-Mitigation Measures

33. Where the level of risk is within a financial institution's risk tolerance, it must ensure that the risk-mitigation measures applied are commensurate with the level of risk identified. Where higher risks are identified, financial institutions must take enhanced measures to manage and mitigate those higher risks.

34. Each financial institution must document its internal controls and related policies and procedures to mitigate and manage the risks it identifies, as well as those identified by the Central Bank, or through any risk assessment carried out at a national level. These policies and procedures must be approved by Senior Management.

35. Some risk mitigation measures include:

i. Determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers, products or a combination of both;

ii. Setting transaction limits for higher-risk customers or products;

iii. Determining the circumstances under which they may refuse to take on or terminate/cease high-risk customers/products or services; and

iv. Determining the circumstances requiring Senior Management approval (e.g., high-risk, or large transactions, when establishing a relationship with high-risk customers such as PEPs).

IV. Evaluate Residual Risk

36. Residual risk is the level of risk remaining after the application of risk-mitigation measures. Regardless of the strength of a financial institution's risk-mitigation methods, there will always be some residual ML/TF risk, which a financial institution must manage. Where the level of residual risk exceeds a financial institution's risk tolerance, or where its mitigation measures do not adequately mitigate high risks, the strength of mitigation measures should be increased.

V. Monitor and Review Risks

37. The risk assessment should be kept up-to-date through periodic reviews and when risk factors change. Financial institutions should ensure that their risk assessment programme is reviewed to assess the implications of:

i. New products, services, practices, technologies and delivery channels;

ii. New ML/TF trends or typologies;

iii. New regulatory guidance;

iv. Changes in customer portfolios or conduct;

v. Changes in products, services and delivery channels;

vi. Changes in business practices; and

vii. Changes in the law.

38. These risk assessments must be made available upon request by the Central Bank. Financial institutions 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, financial institutions must engage an independent audit function to test the internal AML/CFT/CPF policies, controls, and procedures. The independent audit provides an opportunity for each financial institution to consider whether its risk assessments are up to date.

C. New Products, Practices and Technological Developments Risk Assessment

39. Financial institutions must take such measures as may be needed to identify and assess the risks that may arise in relation to:

i. The development of new products and new business practices, including new delivery mechanisms; and

ii. The use of new and developing technologies for new and pre-existing products.

40. Financial institutions must undertake the risk assessment prior to the launch or use of such products, practices, and technologies, and should take appropriate measures, which are commensurate with the identified risks, to manage and mitigate those risks. FI's are also expected to establish a transparent process for product reviews and approvals.

41. Financial institutions offering internet-based and/or telephone products and services should ensure that they have reliable and secure methods to verify the identity of their customers. The level of verification used should be appropriate to the risks associated with the product or service. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their telephone and internet banking applications and, whenever appropriate, they should implement multi-factor verification measures, layered security, or other controls reasonably calculated to mitigate those risks.