CENTRAL BANK OF
TRINIDAD & TOBAGO

Guideline on Anti-Money Laundering and Combatting of Terrorism Financing

This Guideline is being issued pursuant to regulation 40A of the Financial Obligations Regulations, Chapter 11:27 and regulation 3(1) of the Financial Obligations (Financing of Terrorism) Regulations Chapter 12:07 and is intended to assist financial institutions with inter alia complying with Trinidad and Tobago's AML/CFT laws including applying a risk-based AML/CFT approach.

Updated April 13, 2018

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ACO	Alternate Compliance Officer
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and the Combatting the Financing of Terrorism
ATA	The Anti-Terrorism Act, Chapter 12:07
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlement
CDD	Customer Due Diligence
CO	Compliance Officer
CFATF	Caribbean Financial Action Task Force
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIA	Financial Institutions Act, 2008
FIU	Financial Intelligence Unit of Trinidad and Tobago
FIUTTA	The Financial Intelligence Unit of Trinidad and Tobago, Chapter 72:01
FOR	Financial Obligations Regulations
FSRB	FATF-Styled Regional Body
FT/TF	Financing of Terrorism
F/X	Foreign Exchange
GCO	Group Compliance Officer
IA	Insurance Act, Chapter 84:01
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
iSAR	Internal Suspicious Activity Report
ISIL	Islamic State of Iraq and the Levant
KYC	Knowing Your Customer
KYE	Knowing Your Employee
LEI	Legal Entity Identifier
ME	Mutual Evaluation
ML/TF	Money Laundering and Terrorism Financing
NRA	National Risk Assessment
NPO	Non-Profit Organization
OCC	Office of the Comptroller of the Currency
OECD	Organisation for Economic Co-operation and Development
PEP	Politically Exposed Person
POCA	Proceeds of Crime Act and Regulations, Chapter 11:27
PF	Proliferation Financing
PSP	Payment System Provider
SA	Supervisory Authority
SDD	Simplified Due Diligence
STR	Suspicious Transaction/Activity Report
TTSEC	Trinidad and Tobago Stock Exchange Commission
UNCAC	United Nations Convention against Corruption
VAT	Value Added Tax
WMD	Proliferation of Weapons of Mass Destruction

PART I

INTRODUCTION

Part I – Introduction

Money laundering and terrorism financing (ML/TF) continue to be a serious global threat which can adversely affect a country's reputation and lead to dire economic and social consequences, such as de-risking[1]. Internationally, there have been concerted efforts, driven primarily by the Financial Action Task Force (FATF), to implement effective measures to prevent and detect ML/TF.

In 2012, the FATF revised its 40 Recommendations for anti-money laundering and combatting the financing of terrorism (AML/CFT). The FATF Standards/ Recommendations are the global benchmark for assessing the strength and effectiveness of a country's AML/CFT regime. The FATF also added standards for countering proliferation financing (CPF).

A key element of the FATF's revised 2012 Recommendations is the application of a **risk based approach**. Under the risk-based approach, countries and financial institutions are expected to understand, identify and assess their risks, take appropriate actions to mitigate those risks and allocate their resources efficiently by focusing on higher risk areas. Consequently, in 2014, Trinidad and Tobago's AML/CFT legislation was revised to align more closely with the revised FATF Standards. A significant provision in the revised Financial Obligations Regulations (FOR), 2010 (as amended) is the requirement to apply risk sensitive measures based on a comprehensive ML/TF risk assessment taking into consideration the nature, size and complexity of the business.

The Central Bank of Trinidad and Tobago (Central Bank/Bank) first issued an AML/CFT Guideline in 2004 which was subsequently revised in 2005 and 2011. However, it was only in 2010 that the Central Bank was specifically named as a Supervisory Authority[2] (SA) for AML/CFT along with the Trinidad and Tobago Securities and Exchange Commission (TTSEC) and the Financial Intelligence Unit of Trinidad and Tobago (FIU). As an SA, the Central Bank is required to ensure that the financial entities that it regulates comply with the AML/CFT legislation and implement robust AML/CFT frameworks that are commensurate with their size, complexity and risk profile.

In 2015, Trinidad and Tobago was subject to a 4th Round Mutual Evaluation (ME) by the Caribbean Financial Action Task Force (CFATF) to assess compliance with the FATF's revised Standards. The country also conducted a National Risk Assessment (NRA) during 2014/ 2015. Consequently, this revised Guideline seeks to address the findings of the ME and the NRA and to more closely reflect the 2012 revised FATF Recommendations, the Basel Committee on Banking Supervision's guidance[3] and the 2013 FATF's revised Financial Inclusion Guidance[4].

[1] The FATF refers to de-risking as "*situations where financial institutions terminate or restrict business relationships with entire countries or classes of customer in order to avoid, rather than manage risks*." FATF Guidance, Correspondent Banking Services, October 2016.

[2] Definition of a 'Supervisory Authority' in Regulation 2 Financial Obligations Regulations, 2010. The Trinidad and Tobago Securities and Exchange Commission (SEC) and the Financial Intelligence Unit of Trinidad and Tobago are also supervisory authorities for their regulated entities.

[3] BCBS Guidelines - Sound Management of Risks related to Money Laundering and Financing of Terrorism, 2016.

[4] FATF Guidance AML/CFT Measures and Financial Inclusion, revised November 2017

1. LEGISLATIVE FRAMEWORK

The AML/CFT legislative framework is comprised of the following key laws:

- Proceeds of Crime Act and Regulations, Chapter 11:27 (POCA);
- The Anti-Terrorism Act and Regulations, Chapter 12:07 (ATA); and
- The Financial Intelligence Unit of Trinidad and Tobago Act and Regulations, Chapter 72:01 (FIUTTA).

2. OBJECTIVE OF THE GUIDELINE

This Guideline is being issued pursuant to Regulation 40A of the Financial Obligations Regulations, Chapter 11:27 and Regulation 3(1) of the Financial Obligations (Financing of Terrorism) Regulations Chapter 12:07 and is intended to assist financial institutions with:

- Understanding and complying with AML/CFT legislative and regulatory requirements;
- Developing and implementing effective, risk-based AML/CFT compliance programs that enable adequate identification, monitoring and reporting of suspicious transactions; and
- Understanding the expectations of the Central Bank with respect to the minimum standards for AML/CFT controls.

3. SCOPE AND APPLICATION OF THE GUIDELINE

This Guideline applies to:

- Commercial banks and financial institutions regulated under the Financial Institutions Act, Chapter 79:09 (FIA);
- An insurance company, agent or broker[5] registered under the Insurance Act, Chapter 84:01 (IA);
- A person licensed under the Exchange Control Act, Chapter 79:50 (ECA) to operate a Bureau de Change[6];
- Persons engaged in money transmission or remittance business pursuant to Section 36(cc) of the Central Bank Act, Chapter 79:02. This includes agents and sub-agents of money remitters;
- The Home Mortgage Bank established under the Home Mortgage Bank Act Chap 79.08;

[5] The National Risk Assessment concluded that certain classes of insurance, namely general, health and term life, present low ML/TF risk. Additionally, the FATF Standards in respect of the insurance sector apply to the underwriting and placement of life insurance and other investment related insurance. In accordance with a risk based approach, the application of simplified due diligence in instances of low ML/TF risk is acceptable.

[6] See https://www.central-bank.org.tt/core-functions/supervision/bureaux-de-change for list of authorized Bureau de Change Operators.

- The Agricultural Development Bank established under the Agricultural Development Bank Act Chap 79.07; and
- The Trinidad and Tobago Mortgage Finance Company.

Hereinafter in this Guideline, the aforementioned institutions and persons listed are collectively referred to as **financial institutions**.

This Guideline together with the AML/CFT legislation and regulations will form the framework against which the Central Bank will assess the adequacy and effectiveness of financial institutions' AML/CFT compliance programs.

From time to time the Central Bank will amend this Guideline to address changes in the AML/CFT legislative framework. However, financial institutions should as part of their risk management practices, stay current with emerging developments as they relate to AML/CFT and update their AML/CFT programmes as necessary.

This Guideline is divided into five (5) Parts:

- **Part I** is the Introduction and provides information on the objectives, scope and applicability of the Guideline including, transitioning. Part I also includes information on the role of the Central Bank as a SA for AML/CFT.
- **Part II** provides general guidance on AML/CFT Governance and Risk Management for adoption by all financial institutions as appropriate.
- **Part III** provides practical guidance on conducting an ML/TF risk assessment. It is intended to equip financial institutions with the tools needed to assess their ML/TF risk and make informed decisions on the basis of those risk assessments.
- **Part IV** sets out guidance adapted from the Basel Committee on Banking Supervision (BCBS) to assist financial institutions with developing a risk based customer due diligence programme. This Part should be read in conjunction with Part II.
- **Part V** provides examples of risk factors for specific sectors and risk-based application of customer due diligence measures that may be applied. This Part should be read in conjunction with Parts II and IV.

4. EFFECTIVE DATE AND TRANSITION PERIOD

The revised AML/CFT Guideline comes into effect from the date of issue. All regulated entities must conduct a gap analysis against the requirements of the AML/CFT Guideline and submit that gap analysis with an implementation plan to the Central Bank by **July 13, 2018**.

Financial institutions will be required to conduct their **2018 AML/CFT external audits** using the revised AML/CFT Guideline. The Central Bank recognizes that in some instances financial institutions would not have completed their implementation plan by the 2018 audit cycle, however in such instances, the external audit should consider the status of the financial institution's implementation plan in its assessment.

5. THE ROLE OF THE CENTRAL BANK AS THE SUPERVISORY AUTHORITY

The POCA, the FOR and the ATA designate the Central Bank as the AML/CFT SA for the financial institutions listed in this section. The primary responsibilities of the Central Bank as an SA include:

- reviewing the compliance programme of all financial institutions to determine its adequacy and compliance with applicable laws and guidelines;
- approving the Compliance Officer and Alternate Compliance Officer;
- issuing guidelines to aid compliance with AML/CFT requirements;
- receiving and reviewing the financial institution's AML/CFT external audit report annually;
- taking proportionate and dissuasive regulatory action against those financial institutions and persons regulated by it which fail to comply adequately with AML/CFT statutory obligations and guidelines issued by the Central Bank; and
- sharing information with the FIU, SEC and other regulatory agencies as required for the purposes of AML/CFT. This includes disclosing information to the FIU as soon as is reasonably practicable where it has knowledge or has reasonable grounds for believing that a financial institution may have been engaged in money laundering[7] or terrorist financing.

6. ENFORCEABILITY OF THIS GUIDELINE

Further to Regulations 40A and 40 of the FOR, as well as Section 10 of the FIA, the Central Bank is empowered to issue guidelines to aid compliance with the POCA, the ATA or any other written law relating to AML/CFT.

Pursuant to Sections 12 and 86 of the FIA, the Central Bank can issue compliance directions to ensure compliance with this Guideline.

Sections 65 to 67 of the IA allow the Central Bank to issue compliance directions to an insurer or agent, or its controllers or officers for breaching any written law, including AML/CFT laws.

The Terms and Conditions for the Operations of a Bureau de Change (Terms and Conditions) were amended to require Bureaux de Change operators to meet AML/CFT requirements. Non-compliance with the Terms and Conditions can result in the suspension or revocation of a bureau's licence.

[7] Refer to the FOR Regulation 41(1) which applies mutatis mutandis to the Financial Obligations (Financing of Terrorism) Regulations, 2011.

PART II

GENERAL GUIDANCE ON AML/CFT GOVERNANCE AND RISK MANAGEMENT

Part II - General Guidance

This Part should be read in conjunction with the other Parts of this Guideline and is applicable to the financial institutions and persons supervised by the Central Bank as listed in Section 3 of **Part I - Introduction**. Some of the requirements may be adapted by small or specialised institutions, to fit their specific size, business models and sectors.

1. KEY CONCEPTS

1.1 Money Laundering

Money laundering is the process used by criminals to conceal the illegal origin and ownership of funds derived from criminal activities. If successfully undertaken, it allows them to maintain control over those proceeds, the funds loses its criminal identity and appears to be legitimately derived. The money laundering process involves three (3) main stages, namely, placement, layering and integration:

i. **Placement**: refers to the placing of proceeds of crime into the financial system without arousing suspicion, for example via deposits, purchases of cheques or money orders.

ii. **Layering**: refers to the movement of the money, often in a series of financial transactions which may cross multiple jurisdictions designed to disguise the criminal source and provide the appearance of legitimacy. These transactions include purchasing investment instruments, insurance contracts, wire transfers, money orders and letters of credit.

iii. **Integration**: refers to the attempt to legitimize wealth derived from criminal activity. The illicit funds re-enter the legitimate economy by way of investment in real estate, luxury assets and business ventures, until the laundered funds are eventually disbursed back to the criminal appearing to be legitimate funds.

There are three (3) broad groups of offences[8] related to money laundering. These are:

i. Knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of criminal property;

ii. Failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and

iii. Tipping off or prejudicing an investigation.

It is also a separate offence under the POCA[9] not to establish appropriate policies and procedures to detect and prevent money laundering (regardless of whether or not money laundering actually takes place).

[8] Sections 45, 51 and 52 of POCA
[9] Section 57 of POCA

1.2 Terrorism Financing

Terrorism is the unlawful threat of action designed to compel the government or an international organization or intimidate the public or a section of the public for the purpose of advancing a political, religious or ideological belief or cause. Financing of terrorism (FT/TF) is the process by which funds are provided to an individual or group to finance terrorist acts.

The key difference between ML and TF is that with ML, the person seeks to disguise the origins of illicit funds with a profit motive in mind; while in contrast, a person funding terrorism may use legitimately-held funds to pursue illegal and ideological motives. Financial institutions should bear this in mind when assessing the risks posed by those funding terrorism. A financial institution that carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organisations or that the transaction is linked to or is likely to be used in terrorist activity, is committing a criminal offence.

TF often involves small sums of money and may be difficult to detect. Notwithstanding, many of the AML controls financial institutions have in place will overlap with measures to combat the financing of terrorism (CFT). These may include for example, risk assessments, customer due diligence procedures, transaction monitoring and reporting of suspicious activity and transactions. The guidance provided in these Guidelines therefore applies equally to CFT as it does to AML, even where this is not explicitly stated.

Funding for terrorist groups may come from various sources. While state sponsored terrorism has declined in recent years, other types of funding have been observed. Traditional sources include 'revenue-generating' criminal activities such as kidnapping and extortion[10]. Funding may also include income from legitimate sources such as fundraising by charitable or relief organizations. Donors are led to believe that they are giving to support a worthwhile cause and have no knowledge that some or all of the funds donated is being diverted to support terrorism.

In recent times, terrorist groups have occupied territories in different jurisdictions by force and exploited the local population and material resources through extortion, taxation and theft. These include bank looting, control of oil fields and refineries and robbery of economic assets. Technology has also been leveraged to obtain funds through modern communication techniques such as crowd-funding.

1.3 Financing of Proliferation of Weapons of Mass Destruction

The FATF provides a broad working definition for proliferation financing (PF):

"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[11]."

Proliferation of weapons of mass destruction (WMDs) can take many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in

[10] FATF Guidance for Financial Institutions in Detecting Terrorist Financing, April 2002
[11] http://www.fatfgafi.org/topics/methodsandtrends/documents/typologiesreportonproliferationfinancing.html

programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles).

PF poses a significant threat to global security and unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organizations or acting as representatives or middlemen. The FATF Recommendation 7 places obligations on countries to comply with all United Nations Security Council Resolutions to apply targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction. The role of financial institutions is to implement controls to prevent access to financing by individuals and entities who may be involved in or supporting such proliferation. Even though Trinidad and Tobago does not yet have a regulatory framework for proliferation financing, it is recommended that financial institutions' AML/CFT compliance programmes include PF controls, such as screening against the applicable UN lists of designated persons and countries.

2. AML/CFT REQUIREMENTS FOR FINANCIAL INSTITUTIONS

Financial institutions regulated by the Central Bank are required to implement risk-based AML/CFT compliance programmes that are approved by their board of directors. At a minimum, a compliance programme referred to in Regulation 7(1) of the FOR should include the following:

i. Internal systems, processes and controls to ensure ongoing compliance with AML/CFT requirements;

ii. Internal and external audits to verify compliance with AML/CFT requirements;

iii. Training of relevant personnel in the identification, monitoring and reporting of suspicious transactions; and

iv. A Compliance Officer, appointed by Senior Management and approved by the Central Bank, with responsibility for continual compliance with the AML/CFT legislation and guidelines.

3. AML/CFT GOVERNANCE FRAMEWORK

ML and TF prevention should not be viewed in isolation from a financial institution's other business systems and needs, but as part of the institution's overall risk management strategies. Consequently, it is imperative that the board and senior management of financial institutions ensure that the policies, procedures, systems and processes that are put in place to prevent ML/FT and PF as appropriate. The financial institution's AML/CFT programme should be risk-based and commensurate with the nature, size, complexity and inherent risks of their financial institution.

In accordance with the Three Lines of Defense Model[12], business units (e.g. customer-facing functions) constitute the first line of defense with responsibility for identifying, assessing and controlling the ML/TF risks of their business. The financial institution's AML/CFT policies, procedures and controls must be clearly documented and communicated to all relevant employees in

[12] Institute of Internal Auditors, Position Paper, *The three lines of defence in effective risk management and contro*l, January 2013. The Model has become the most common benchmark for assigning control and risk management responsibilities to business functions in an organisation.

the business units. All employees must be adequately trained to implement the AML/CFT policies and procedures and to be aware of their obligations in ensuring compliance with prevailing AML/CFT laws, regulations and guidelines.

The compliance function and other control functions comprise the second line of defense and is responsible for ongoing monitoring of the financial institution's compliance with AML/CFT requirements. This includes sample testing and the review of exception reports to identify potential compliance breaches by the financial institution. The Compliance Officer of a financial institution also has statutory responsibility for reporting suspicious activity and transactions and must be provided with adequate resources to effectively execute the compliance functions as prescribed in regulation 4 of the FOR.

Internal Audit is charged with the third line of defense and should be separate from both the first and second lines of defense. Internal Audit is responsible for independent oversight and evaluation of the financial institution's AML/CFT risk management controls, processes, systems and of the effectiveness of the first and second line of defense functions. Findings of such reviews must be reported to the audit committee of the Board or an equivalent oversight body.

Further, there are additional external levels of control that complement the three (3) internal lines of control[13]. External auditors and the designated SAs are the most common and play a critical role in independently assessing the financial institution's overall governance and control structure to determine whether it is adequately complying with the relevant standards and rules. External auditors are required by law to conduct an annual AML/CFT audit on all regulated entities and submit reports to the respective SA. The SAs issues guidance to regulated entities and also assess their compliance with regulatory rules and standards.

3.1 Role of the Board of Directors (Board)

The Board has overall accountability for ensuring the effectiveness of the AML/CFT compliance program. In this regard, the Board's oversight in respect of AML/CFT should align with international best practices, including the Central Bank's Corporate Governance Guideline and in particular, Section 12.1.1 "*The Role of the Board in Risk Management*". The Board must ensure that there is documented evidence of its oversight function, for example, in minutes of meetings of the Board (or committees of the Board).

Key responsibilities of the Board include:

i. Approving the AML/CFT compliance programme including all AML/CFT policies;

ii. Ensuring the establishment of appropriate mechanisms to periodically review key AML/CFT policies and procedures to ensure their continued relevance in line with changes in the financial institution's products and services and to address new and emerging ML/TF risks;

iii. Ensuring the establishment of an appropriate AML/CFT risk management framework with clearly defined lines of authority and responsibility for AML/CFT

[13] The Financial Stability Institute, *The "Four lines of defense model" for Financial Institutions*, Occasional Paper No. 11, December 2015 proposes a fourth line of defense which comprises the regulators and external auditors both of whom have a key role to play in ensuring effective corporate governance and risk management of financial institutions.

and effective separation of duties between those implementing the policies and procedures and those enforcing the controls;

iv. Ensuring that the Board receives the requisite training on AML/CFT generally as well as on the institution's specific AML/CFT risks and controls;

v. Ensuring receipt of regular and comprehensive reports on the financial institution's AML/CFT risks from the CO and/or other senior officers, including but not limited to:

- Remedial action plans if any, to address the results of independent audits (either internal or external); regulatory reports received from the Central Bank or other regulators on its assessment of the institution's AML/CFT program; and results of compliance testing and self-identified instances of non-compliance with AML/CFT requirements;
- Recent developments in AML/CFT laws and regulations and implications if any, to the financial institution;
- Details of recent significant risk events and potential impact on the financial institution; and
- Metrics including but not limited to, statutory reporting to the FIU, orders from law enforcement agencies, refused or declined business and de-risked relationships.

3.2 Role of Senior Management

Senior Management is responsible for the day-to-day implementation, monitoring and management of the financial institution's AML/CFT compliance programme, including ensuring adherence to established AML/CFT policies and procedures. Among other things, Senior Management should ensure that policies and procedures:

i. Are risk based, proportional and adequate to mitigate ML and TF risks of the financial institution;

ii. Comply with all relevant AML/CFT laws, regulations and guidelines; and

iii. Are implemented effectively across relevant business areas or throughout the financial group as applicable.

Senior Management must review policies and procedures periodically for consistency with the financial institution's business model, product and service offerings, and risk appetite. Attention should be paid to **new and developing technologies** and financial institutions should identify and assess the ML/FT risks arising from **new products/services and delivery channels; new business practices and new or developing technologies for new and existing products; and put measures in place to manage and mitigate such risks**. Risk assessments should take place prior to the launch or use of such products/services, channel, business practices and technologies.

Senior Management should also ensure that:

i. All significant recommendations made by internal and external auditors and regulators in respect of the AML/CFT program are acted upon in a timely manner;

ii. Relevant, adequate and timely information regarding AML/CFT matters is provided to the Board;

iii. The CO and their alternate receive the appropriate training on an ongoing basis to effectively perform his duties;

iv. There is an ongoing employee training programme which enables employees to have sufficient knowledge to understand and discharge their AML/CFT responsibilities; and

v. The Compliance and Internal Audit functions are resourced adequately in terms of people, IT systems and budget to implement, administer and monitor the AML/CFT program requirements effectively.

3.3 Role of the Compliance Officer[14]

Every financial institution shall for the purpose of securing compliance with Section 55(A) of POCA and Regulation 3 of the FOR, designate a manager or official employed at a managerial level as the CO[15] of that institution[16]. The CO must be approved by the Central Bank and must satisfy the definition of an "officer" as contained in the respective legislation[17] that governs financial institutions. Accordingly, the CO must satisfy the "fit and proper" requirements outlined in the Central Bank's Fit and Proper Guideline.

Financial institutions shall inform the Central Bank in writing, within **one (1) week** of the appointment or change in the appointment of the CO and submit the necessary documentation for approval to the Central Bank. The financial institution should also advise the FIU of the CO.

Where a financial institution is also registered with the TTSEC, the financial institution must submit applications for the approval of a CO simultaneously to each SA. The application to each SA should indicate that an application was also submitted to the other SA. The SAs will consult with each other on the suitability of the applicant and responses will be conveyed by each SA to its respective licensee or registrant.

Where a financial institution has five (5) or fewer employees, as may be the case with an insurance broker, bureau de change or money remittance company, the most senior employee shall be the CO[18]. Where the financial institution is part of a financial group, consideration may be given to the suitability of an applicant from within the group, provided that appropriate service level arrangements are in place.

As far as is practical, the CO must have sufficient authority, independence and seniority to be able to effectively carry out his duties in accordance with the FOR. The identity of the CO must be treated with strictest confidence by the employees of the institution.

The CO must have the necessary knowledge and expertise to effectively discharge his role and responsibilities, including keeping abreast of the latest developments in ML/TF techniques and the

[14] The functions of a compliance officer are outlined in Regulations 4 and 8 of the FOR.
[15] A Compliance Officer is defined in Part I of the FOR.
[16] Refer to the FOR, Regulation 3.
[17] See Interpretation section of the FIA and the IA.
[18] Refer to the FOR, Regulation 3(3).

AML/CFT best practices within the industry. Consequently, the CO should possess professional qualifications/ certification in AML/CFT. Notwithstanding, on an ongoing basis financial institutions must ensure that the CO and other staff receive specialized training that is appropriate to their particular job function so that they are able to effectively discharge their duties. Specialized training on the prevention and detection of ML/FT include, but is not limited to:

i. AML/CFT legislative and regulatory requirements;
ii. the FATF 40 Recommendations, including ML/TF typologies;
iii. the identification, assessment and management of ML/FT risk;
iv. the design and implementation of risk based internal systems of AML/CFT control;
v. the design and implementation of AML/CFT compliance testing and monitoring programs;
vi. review and handling of internal unusual or suspicious activity reports;
vii. the identification and handling of completed and attempted suspicious activity and transactions;
viii. the process for submitting a suspicious activity or transaction report to the FIU;
ix. the handling of Monitoring, Production and Restraint Orders received from law enforcement agencies;
x. the ML/TF vulnerabilities of relevant services and products;
xi. ML/TF trends and typologies; and
xii. managing 'tipping off' risk.

Good governance practices require that the CO should be independent of the receipt, transfer or payment of funds, or management of customer relationships and assets. In considering the independence of the CO, consideration should be given to any potential conflicts of interest that may arise between the compliance function and any other responsibilities discharged by the CO. In determining independence the following should be taken into account:

i. *The nature of the reporting lines between the CO and management of operating/business units.* Ideally, the CO should have a direct reporting line to senior management and where necessary to the Board of Directors (or relevant Committee of the Board) of the institution. The CO should not have a reporting line to a senior manager with business line responsibilities. For smaller companies where independence may not be practical, consider administrative reporting to a business line manager and functional reporting to a more senior officer or to the Board. Ultimately, the financial institution must be able to demonstrate the independence of the CO in form in instances where practically, independence cannot be achieved functionally.
ii. *Potential conflicts of interest between their compliance responsibilities and any other responsibilities that the CO may have*. In general, the CO should not have any other responsibilities than that of compliance. However, where this is not feasible, institutions should make appointments that as far as possible, avoid conflicts of interest.

iii. *The remuneration structure*. Institutions should ensure that remuneration of the CO is not related to the performance of any one business line within the organization.

For consistency and to ensure ongoing attention to the compliance regime, the appointed CO may delegate certain duties to other employees. However, where such a delegation occurs, the CO retains responsibility and accountability for the compliance programme. The CO must have:

i. Unfettered access to, and direct communications with Senior Management and the Board; and

ii. Timely and uninhibited access to customer identification, transaction records and other relevant information throughout the organization.

3.4. Responsibilities of the CO

The CO has overall responsibility for the implementation of the AML/CFT programme. At a minimum, the CO must perform the functions and duties as prescribed in Regulation 4(1) of the FOR and among other things should:

i. Have oversight of the AML/CFT control activity in all relevant business areas for the purposes of establishing a reasonable threshold level of control consistency throughout the financial institution;

ii. Keep the AML/CFT program current relative to the institution's identified inherent risks and giving consideration to local and international developments in ML and TF;

iii. Conduct regular risk assessments of the inherent ML and TF risks including timely assessments of new products, services and business acquisition initiatives to identify potential ML/TF risks and develop appropriate control mechanisms;

iv. Conduct periodic assessments of AML/CFT control mechanisms to ensure their continued relevance and effectiveness in addressing changing ML/TF risks, assess operational changes, including the introduction of new technology and processes to ensure that ML/TF risks are addressed;

v. Ensure systems resources, including those required to identify and report suspicious transactions and suspicious attempted transactions, are appropriate in all relevant areas of the institution;

vi. Develop written AML/CFT policies and procedures that are kept up to date and approved by the Board;

vii. Ensure that ongoing training programs on ML and TF are current and relevant and are carried out for all employees, senior management and the Board;

viii. Ensure that systems and other processes that generate information used in reports to Senior Management and the Board are adequate and appropriate, use reasonably consistent reporting criteria, and generate accurate information; and

ix. Report pertinent information to the Board and Senior Management regarding the adequacy of the AML/CFT framework or any associated issues.

3.5 The Alternate Compliance Officer (ACO)

Financial institutions are required to appoint an officer as an alternate to the CO in accordance with Regulation 3(8) of the FOR. The ACO should have the same responsibilities as the CO, during periods of prolonged absences by the CO, such as vacation and sick leave. Consequently, all requirements and responsibilities stipulated for the Compliance Office under Sections 3.3 and 3.4 apply equally to the ACO.

4. INDEPENDENT TESTING

Financial institutions must conduct independent testing of the compliance programme[19]. It is important that these reviews are performed by auditors who have had appropriate AML/CFT training and experience in respect of ML and TF risk and an appropriate level of knowledge of the regulatory requirements and guidelines. Where a financial institution fails to engage the services of an external or internal auditor, the Central Bank shall appoint a competent professional to perform those functions and the costs shall be borne by the financial institution.[20.]

4.1 External Audits

Reviews of the financial institution's AML/CFT policies, procedures and processes for compliance with legislation must be conducted annually[21]. The external audit report in the approved ICATT format[22] must be submitted to the Central Bank and the financial institution's Board within four (4) months of the financial institution's year end.

External audits of insurance companies with agency arrangements must include a sample of business introduced by incorporated agents of the insurance company. The external auditor should also assess the controls put in place by the insurance company to ensure that the agents comply with the company's compliance programme and that agents are included in the insurance company's AML/CFT training.

4.2 Internal Audits

The Internal Auditor should perform regular reviews to evaluate the adequacy of implementation of the financial institution's AML/CFT policies, procedures and systems. The Central Bank may also request that a financial institution conduct an internal AML/CFT audit if, in the Central Bank's opinion, such an audit is warranted. The frequency of internal audit review may be determined by the financial institution commensurate with its complexity, size and risk profile, but at a minimum should be conducted every three (3) years. The basis for the audit frequency must be clearly articulated in the financial institution's audit policy and scope.

The review process should identify weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions, including ensuring that recommendations made by the external auditor and the Central Bank have been satisfactorily addressed.

19 Refer to the FOR Regulation10.
20 Refer to the FOR Regulations 10(3) and 10(4).
21 See FOR Regulation 10(2)(a) for scope of external audit.
22 The Institute of Chartered Accountants of Trinidad and Tobago (ICATT) worked with the Central Bank, TTSEC and the FIU to agree a format for external audits reviews of financial institutions' AML/CFT compliance programme.

The internal audit should also review the risk assessment carried out by the institution to ensure that it is sufficiently comprehensive. The adequacy of the compliance programme should also be reviewed to ensure that it is effectively mitigates any identified risks.

Auditors should document the audit scope, procedures performed, transaction testing completed, and findings of the review. All audit documentation should be made available for Central Bank's review upon request. Any breaches, policy or procedure exceptions or other deficiencies noted during the audit should be documented in an audit report and reported to senior management and the Board or a designated committee in a timely manner. Senior management should advise on corrective actions to address deficiencies and a timeline for implementing such actions. The Board or designated committee and audit should track audit deficiencies and ensure that corrective actions are implemented in a timely manner.

The internal audit would include, *inter alia:*

i. A review of the financial institution's risk assessment and risk rating process for reasonableness given its risk profile (services, customers and geographic locations (both of the business and its customers' locations));

ii. Determining the adequacy of the financial institution's ML/TF risk assessment framework and application of a risk-based approach in the design of its AML/CFT policies, procedures and controls;

iii. Appropriate risk-based transaction testing to verify adherence to the AML/CFT recordkeeping and reporting requirements;

iv. An evaluation of management's efforts to resolve breaches and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable;

v. A review of employee training for effectiveness, completeness and frequency and the extent of employees' and officers' (including senior management's) compliance with established AML/CFT policies and procedures;

vi. A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for AML/CFT compliance including a review of the criteria and processes for identifying and reporting suspicious transactions;

vii. An assessment of the overall process for identifying and reporting suspicious activity, including a review of 'not filed' (closed not suspicious) internal suspicious transactions/activity reports to determine the adequacy, completeness and effectiveness of the adjudication process. It should be noted that the internal audit review does not include a review of actual SAR/STRs filed with the FIU.

The internal audit review should include interviews with key employees, such as staff of the compliance unit, customer facing employees handling transactions and their supervisors to determine their knowledge of the AML/CFT legislative requirements and the financial institution's policies and procedures.

5. AML/CFT RISK MANAGEMENT

5.1 Risk Based AML/CFT Compliance Programmes

Having a risk-based approach to AML/CFT is essential for the implementation of an effective AML/CFT risk management framework and the promotion of financial inclusion. The risk based approach allows for the implementation of appropriate customer due diligence, verification and monitoring procedures that are proportionate to the identified ML/TF risks that the financial institution is exposed to from its customers, products and countries with which it transacts business.

FATF recognizes that a regime that is risk based will not be a 'zero failure' regime. However, the Central Bank must be satisfied that the financial institution is generally taking reasonable measures to identify, monitor, control and report its ML/TF risks.

The Central Bank recognizes that the relationship between a customer and a financial institution is contractual and the decision to accept or maintain a business relationship has a commercial basis. However, 'de-risking' or terminating or restricting business relationships with customers or categories of customers without adequately assessing the risk and considering options to manage the risk, is not in keeping with a risk based approach[23]. An overly cautious approach to AML/CFT measures may have the unintended consequence of excluding legitimate businesses and consumers from the formal financial system. Such actions may also lead to an overall reduction in financial sector transparency, creation of obstacles to trade, contribute to financial exclusion and drive financial transactions underground. Further information on the subject of de-risking is available at the following link: FATF Clarifies the Risk Based Approach.

The risk-based approach requires financial institutions to implement measures to mitigate the risks identified from its enterprise business risk assessment that are appropriate for the nature, size and complexity of the financial institution. Section 2 of this Part identifies the minimum components of a risk based compliance programme.

5.2 AML/CFT Compliance Programmes of Financial Groups

Financial institutions or financial holding companies with branches or subsidiaries either in, or outside of Trinidad and Tobago, should implement a group-wide AML/CFT compliance programme[24]. The parent of the financial group must establish appropriate oversight and reporting structures to ensure that group wide policies and procedures are communicated, implemented and monitored across all branches and subsidiaries and elements of the business that have been outsourced.

Policies and procedures should not merely comply with all relevant laws and regulations, but should appropriately identify, monitor and mitigate group-wide risks. In this regard, financial institutions should monitor significant customer relationships and their transaction activity on a consolidated basis. Group policies and procedures should include a process for identifying, monitoring and investigating unusual activities and transactions and for reporting of suspicious activity and transactions.

[23] CB-OIFI-1655/2015 dated July 10, 2015
[24] Regulation 7(3) of the FOR

Many financial groups offer a range of financial services other than deposit-taking and lending, such as insurance and securities services. Such groups should consider the different risk factors posed by each business line and its customers and have the ability to monitor and share information on the identity of customers and their transactions and account activities across the entire group.

To facilitate group-wide risk assessment and management, the financial institution must also establish and maintain policies, controls and procedures for data protection and sharing of information for the purposes of preventing money laundering and terrorist financing with other members of the group. Such measures should consider the different types of information that may be shared and the requirements for sharing, storage, retrieval and disposal of information.

Where the AML/CFT requirements of the host jurisdiction are of a higher standard, the subsidiary must apply the higher standard. However, where the minimum AML/CFT requirements of the host country are less stringent than that of Trinidad and Tobago, the subsidiary should apply the Trinidad and Tobago requirements to the extent that the host jurisdiction's laws and regulations permit. In accordance with the FATF Standards[25] where the host country's laws either do not meet the FATF Standards or prohibit the implementation of AML/CFT measures that are consistent with Trinidad and Tobago's standards, the financial institution is required to apply appropriate controls to manage ML/TF risks and to report to the Central Bank on the AML/CFT gaps in that jurisdiction and the measures taken to mitigate the risks. The Central Bank will then make a determination on the required course of action which may include the regulatory requirement of closure of the respective foreign subsidiary.

5.2.1 Group Compliance Officer (GCO)

Financial groups should appoint a suitably qualified Group Compliance Officer[26] (GCO) with responsibility for the group wide AML/CFT programme and to ensure its effective implementation. The GCO shall be approved by the Central Bank as an 'officer' in accordance with the Central Bank's Fit and Proper Guideline[27]. The GCO should have the necessary authority such that issues raised by this officer receive the necessary attention from the board, senior management and business lines.

As part of a consolidated risk management approach, the GCO has the overall responsibility for designing and coordinating the implementation of a single AML/CFT strategy across the group. This includes implementation of mandatory policies and procedures. The GCO is responsible for supervising the activities of other compliance function staff, including the designated Compliance Officers. In addition to providing consolidated group oversight, the GCO may be the CO or the ACO of an entity within the financial group.

The GCO should have the ability to monitor and evaluate the ML/TF risk posed by a particular customer or category of customers within the group. Policies and procedures should include management of group relationships that have been deemed high risk, including procedures for escalation and restrictions and/or termination of accounts or relationships.

[25] Interpretive Note to Rec 18 in the FATF Standards
[26] BCBS Sound Management of Risks related to Money Laundering and Financing of Terrorism
[27] https://www.central-bank.org.tt/content/legislation-guidelines-and-letters-0

The GCO should report to the financial institution's parent Board on the adequacy of the group's AML/CFT programme; concerns with and recommendations for high risk relationships; any issues and material changes with remedial actions and milestones; adequacy of resources supporting the programme; and make recommendations regarding the overall structure of the programme as necessary. The GCO should also provide feedback to the COs of the individual financial entities in the group on observed emerging typologies, trends and risk across the group.

5.3 Identifying and Understanding ML/TF Risks

In order to develop a risk based AML/CFT compliance programme, a financial institution must first conduct a risk assessment[28] to understand its risks. Risk assessments should help financial institutions understand the inherent ML/TF risk exposure and which areas of their business they should prioritise in the fight against ML/TF. The risk assessment should be approved by the Board and form the basis for the development of policies and procedures to mitigate ML/TF risks. It should reflect the risk appetite of the institution and establish the risk level deemed acceptable. During an on-site examination, the Central Bank will request and evaluate the adequacy of the financial institution's risk assessment.

Financial institutions shall also incorporate the results of the National Risk Assessment (NRA) where available into their ML/TF risk assessment process and apply the appropriate simplified or enhanced measures commensurate with the identified risks. Guidance on conducting risk assessments is provided in Part III of this Guideline.

5.4 Ongoing Monitoring and Review of ML/TF Risks

The assessment of ML/TF risk is not a static exercise and assessments must be reviewed and updated at appropriate times. Risks that have been identified may change or evolve over time due to any number of factors, including shifts in customer conduct, the development of new technologies and changes in the market. Emerging risks observed from suspicious activity/transaction reports, compliance breaches or intelligence from front-line employees that have a bearing on the risk assessment should be noted and reflected in the risk assessment as soon as possible.

In the absence of material trigger events, financial institutions should re-assess their ML/TF risks at least every three years and may consider setting a mandatory date for review. Material trigger events include business expansion through mergers and acquisitions or introduction of new products and services as a result of new and developing technologies.

In addition to keeping risk assessments up to date and relevant, financial institutions must monitor transactions to ensure that these are in line with the customer's risk profile and business and where necessary, examine the source of funds to detect possible ML/TF. Documents, data or information must be kept up to date on a risk-sensitive basis, with a view to understanding whether the risk associated with the business relationship has changed.

The review of the risk assessment should be documented to evidence that an appropriate review has taken place. The internal sign-off procedure in relation to customer risk assessments should be appropriate to the level of risk.

[28] Regulation 7(2) of the FOR

Customer risk assessments should be reviewed at least annually for higher risk customers. A material change in a customer's circumstances should also prompt a review. Examples of a material change include but are not limited to:

i. Establishing connections with a higher risk jurisdiction or engaging in a higher risk business;

ii. Changes in patterns of transactional activity; and/or

iii. Changes in the nature of the business relationship, control structure or beneficial ownership of customers.

Where a customer has been assessed as posing a higher ML/TF risk and the financial institution is not satisfied that it can effectively mitigate those risks, it may decline entering into a business relationship, carrying out an occasional transaction for that customer or continuing the business relationship. In those instances, where there are reasonable grounds to suspect that money laundering or terrorist financing is being attempted, the financial institution must report this to the FIU.

6. KNOWING YOUR CUSTOMER (KYC) AND CUSTOMER DUE DILIGENCE

Financial institutions must develop and implement risk based policies and procedures to mitigate the ML/TF risks identified in their business and customer risk assessments. The risk assessment framework should identify which customers or categories of customers present higher risk and therefore require the application of enhanced due diligence (EDD). Similarly, where the financial institution determines that a customer or a category of customer presents low risk, simplified due diligence (SDD) should be applied. Where SDD measures are applied on the basis of an assessment of low ML/TF risk, the customer due diligence (CDD) policies and procedures should clearly articulate the rationale and the applicable measures to be undertaken. In this regard, **at a minimum** CDD measures must:

i. Identify the customer and where applicable, the customer's beneficial owner or legal representatives;

ii. Verify the customer's identity on the basis of reliable and independent sources and where applicable, verify the beneficial owner's identity in a way that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer;

iii. Understand and as appropriate, obtain information regarding the purpose and intended nature of the business relationship; and

iv. Conduct ongoing due diligence on the business relationship and scrutinize transactions throughout the relationship to ensure that the activity is consistent with the financial institution's knowledge of the customer and its risk profile, including where applicable, the source of funds.

Financial institutions are required to conduct CDD on the customer and where applicable, the beneficial owner and the person acting on behalf of the customer at appropriate times such as when a customer is attempting to:

i. Establish a business relationship;

ii. Conduct a one-off or occasional transaction of TTD 90,000 or more, where the transaction is carried out in a single operation or in several operations that appear to be linked; or

iii. Conduct a one-off or occasional wire transfers above TTD 6,000 where the transaction is carried out in a single operation or in several operations that appear to be linked.

Financial institutions may also conduct CDD where:

i. There is suspicion of ML/TF, regardless of the amount of the transaction, unless doing so results in tipping off the customer. In such instances, the financial institution may forego the CDD and must file an STR;

ii. There is doubt about the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

CDD should also be conducted when there is a change in the circumstances of the customer, for example, changes to the customer's transaction activity.

The primary purpose of the CDD process is to ensure that the financial institution knows its customers and understands their financial activities. There should be sufficient information to obtain a complete picture of the risk associated with the business relationship and provide a meaningful basis for subsequent monitoring.

The guidance contained hereafter in this Part are consistent with the FATF's guidance on AML/CFT and Financial Inclusion and embodies the BCBS Guidelines[29] particularly with respect to account opening. Part IV of this Guideline provides further guidance on the practical application of the principles set out in the following paragraphs.

6.1 Customer Identification and Verification

The identity of customers, beneficial owners, as well as persons acting on their behalf should be verified using reliable, independent source documents, data or information. Financial institutions should be aware that the best documents for the verification of identity are those most difficult to obtain or counterfeit.

It is important to distinguish between **identifying the customer and verifying identification**. Customer identification entails the gathering of information on the prospective customer to enable identification and includes for example, obtaining information on his/her given/legal name (which may change), residential address (which may change), nationality, date and place of birth and physical appearance. At this stage, there is no collection of identification documents. Other facts about an individual will emerge over time for example, family circumstances; changes in address, employment and business career; contact with the authorities or with other financial institutions. The identity of a

[29] BCBS Guidelines – Sound Management of Risks related to Money Laundering and Financing of Terrorism 2016

customer who is a legal person is a combination of its constitution, its business and its legal and ownership structure.

Verification of the customer identification entails checking reliable, independent source documentation such as photo IDs, birth certificates, data or information that confirms the veracity of the information obtained during the identification process.

Prior to establishing a business relationship, the financial institution should ensure that the customer's identity has been verified. The customer's physical identity should be verified using **one (1) form** of photo ID which may be a valid passport, national identification card **or** driver's license. Additional picture identification should be requested by the financial institution **only** where higher risk is identified and enhanced due diligence is warranted. Based on its risk tolerance and internal policies a financial institution may choose to apply a higher standard to that articulated in this Guideline. In such instances, the financial institution should ensure that their policies and procedures do not exclude vulnerable groups such as low income customers, the elderly, students and small businesses.

In certain circumstances, the FATF Standards[30] allow financial institutions to verify the identity of the customer following the establishment of a business relationship (and not before or during the course of establishing a business relationship), provided that money laundering and terrorist financing risks are effectively managed. Examples of such instances are provided in Section 6.3.1 of this Part.

When commencing a business relationship, the purpose and reason for establishing the business relationship should be recorded, and the anticipated level and nature of activity to be undertaken. The extent of documentary evidence required will depend on the applicant and the nature of the applicant's business. Documentation confirming the nature of the applicant's business (e.g. audited financial statements) or the applicant's occupation (e.g. job letter or last pay slip) may be obtained also to confirm the origin or source of funds to be used during the relationship. Part IV describes types of information that may be collected and verified for individuals and legal persons and arrangements wishing to establish business relationships with a financial institution.

Where a prospective customer fails or is unable to provide adequate evidence of identity or, in instances where the financial institution is not satisfied that the transaction for which it is or may be involved is legitimate, an explanation must be obtained and a decision made by the CO as to whether:

i. It is appropriate to proceed with the business relationship; or
ii. Other measures may be taken to verify the client's identity; and
iii. A report to the FIU should be made.

Financial institutions are prohibited from opening anonymous accounts or accounts in fictitious names. Where a financial institution is unable to verify the true identify of a prospective client or beneficial owner, the financial institution is prohibited from establishing the business relationship, or if already established must immediately terminate the business relationship and consider filing an STR.

[30] INR. 10 para 11, FATF Recommendations, 2013

6.2 Risk Based Customer Due Diligence

While CDD measures are an important component of a robust AML/CFT framework, it is important to strike a balance between the objectives of ensuring financial inclusion and addressing ML/TF risks in a risk sensitive manner. **It is important that a financial institution's CDD policy is not so restrictive or inflexible that it results in a denial of access to basic financial services, especially for those who are economically or socially vulnerable such as low-income groups, the elderly, the disabled, students and minors.** This flexibility is relevant for financial inclusion since the vulnerable population find entry into the regulated financial system difficult as they often do not possess the required identification documents.

6.3 Lower Risk/Simplified Due Diligence

With a risk based approach, where the identified ML/TF risks are lower, financial institutions may apply SDD. SDD should be commensurate with the identified lower risk factors (e.g. the simplified measures may relate only to customer acceptance measures or to aspects of ongoing monitoring). It should be noted that SDD never means a complete exemption or absence of CDD measures but rather, financial institutions may adjust the frequency and intensity of measures to satisfy the minimum CDD standards. Financial institutions are reminded that simplified measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or where specific higher risk is determined.

With respect to beneficial ownership in a financial inclusion context, the beneficial owner will in most instances be the customer himself or a closely related family member. Where there is suspicion that the account owner is being used as a 'strawman' and is not the beneficial owner, normal or enhanced due diligence measures should be applied and an internal suspicious report must be filed with the CO.

The FOR identifies the specific instances[31] when SDD measures may be applied including where lower risks have been identified through a national risk assessment or through an adequate assessment of ML/TF risk by the financial institution. Where the assessment identifies lower ML/TF risk, the financial institution may also apply SDD measures in the following instances, unless there is a suspicion of money laundering or terrorist financing:

i. One-off transactions or occasional transactions below TTD 90,000;
ii. Two or more one-off transactions which together total **less than** TTD 90,000 and which appear to be linked;
iii. One-off wire transfers **less than** TTD 6,000; and
iv. Two or more one-off wire transfers which appear linked and which in total are **less than** TTD 6,000.

In addition, financial institutions may, based on their risk assessments, apply SDD to specifically defined lower risk customers or products and services. Such instances may include but are not limited to:

[31] Regulations 14(1) and 14(3) of the FOR

i. Customers whose sole source of funds is a salary credit to an account or with a regular source of income from a known source which supports the activity being undertaken;

ii. Pensioners, social benefit recipients or customers whose income originates from their spouses'/partners' employment);

iii. Financial products or services that provide appropriately defined and limited services to certain types of customers. For customers who do not have photo identification or have limited identification documentation such as tourists or those who are socially or economically vulnerable such as the disabled, elderly, minors or students, a 'tiered' CDD approach allows financial access with limited functionality. For example, a financial institution may offer banking accounts with low transaction/payment/balance limits with reduced documentation requirements. Access to additional services such as higher transaction limits or account balances or access to diversified delivery channels should only be allowed if and when the customer can satisfy additional identification requirements. Where this obtains financial institutions must have monitoring systems to ensure that transaction and balance limits are observed;

iv. Customers represented by those whose appointment is subject to court approval or ratification (such as executors or receivers).

6.3.1 Examples of SDD Measures

The SDD measures described below are for guidance only and should not be considered as prescriptive or exhaustive. Where a financial institution determines, based on its risk assessment that the ML/TF risks are lower, the financial institution may apply one or more of the following SDD measures:

i. *Adjust the timing of CDD where the product or transaction has features that limit its use for ML/TF purposes.*

Financial institutions may verify the customer's or beneficial owner's identity after the establishment of the business relationship where financial products or services provided have limited functionality or restricted services to certain types of customers for financial inclusion purposes. For example, limits may be imposed on the number or total value of transactions per week/month; the product or service may only be offered to nationals or only domestic transactions may be allowed. Verification of identity may occur when the transaction threshold or time limit is met.

Similarly, general insurance products such as car insurance present low ML/TF risk so verification of identity may be postponed until there is a claim or until the customer requests additional insurance products. In such instances, financial institutions must ensure that:

- This does not result in a de facto exemption from CDD and that the customer or beneficial owner's identity will ultimately be verified.
- The threshold or time limit is set at a reasonably low level;

- Systems are in place to detect when the threshold or time limit has been reached; and
- CDD is not deferred or obtaining relevant information about the customer is not delayed where higher risk factors exist or where there is suspicion of ML/TF.

ii. *Adjust the quantity of information requested from the customer for identification, verification or monitoring purposes.*

Customers warranting SDD based on their risk profile should not be required to produce two (2) forms of ID as a minimum requirement. Financial institutions may:

- Verify identity on the basis of one document only; or
- Assume the nature and purpose of the business relationship because the product is designed for one particular use only, such as a company pension scheme.

iii. *Adjust the quality or source of information obtained for identification, verification or monitoring purposes*

Where the risk associated with all aspects of the relationship is very low, financial institutions may rely on the source of funds to meet some of the CDD requirements, for example, the purpose and intended nature of the relationship may be inferred where the sole inflow of funds are government pension or benefit payments.

iv. *Adjust the frequency of CDD updates and reviews of the business relationship*

This may be applied for example when trigger events occur such as the customer requesting a new product or service or when a certain transaction threshold is reached. Financial institutions must ensure that this does not result in a de facto exemption from keeping CDD information up-to-date.

v. *Adjust the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only*.

Where financial institutions choose to do this, they must ensure that the threshold is set at a reasonable level and that systems are in place to identify linked transactions which, when aggregated, exceed the threshold.

6.4 Higher Risk/Enhanced Due Diligence

Financial institutions are required to apply EDD for such categories of customers, business relationships or transactions that are determined to present higher ML/TF risk due to business activity, ownership structure, nationality, residence status, politically exposed status or other higher risk indicators.

The financial institution's policy framework should therefore include a description of the type of customers that are likely to pose higher than average risk and the EDD procedures to be applied in such instances. The commencement of a business relationship with a high risk customer must be approved by senior management. Senior management should receive sufficient information to make

an informed decision on the level of ML/TF risk the institution would be exposed to if it enters into or continues that business relationship and how well equipped it is to manage that risk effectively.

Financial institutions should also ensure that monitoring systems are appropriately tailored and provide timely and comprehensive reports to facilitate effective monitoring of such relationships and periodic reporting on such relationships to senior management and the Board.

The POCA and the FOR[32] identify specific instances[33] that financial institutions must always treat as high risk and to which EDD must be applied. EDD must be applied in the following circumstances:

i. Business transactions with persons and financial institutions in or from other countries which do not or insufficiently comply with the FATF Standards;

ii. Complex, unusual or large transactions, whether completed or not, to all unusual patterns of transaction and to insignificant but periodic transactions which have no apparent economic or visible lawful purpose;

iii. Where money laundering risks are higher;

iv. When establishing correspondent banking relationships;

v. Where the customer is a foreign politically exposed person (PEP);

vi. Where higher risks have been identified with a customer who is a domestic PEP or a PEP associated with an international organization; and

vii. Non face-to-face business relationships or transactions.

Financial institutions should exercise due caution if entering into business relationships or otherwise doing business with persons from high risk jurisdictions named in Public Statements issued by the FATF, CFATF and FATF styled regional bodies.

6.4.1 Examples of EDD Measures

When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, examples of EDD measures include (but are not limited to) ***taking more intrusive and exhaustive steps*** to:

i. Increase the quantity of information obtained for CDD purposes (e.g. request additional information as to the customer's residential status, employment, salary details and other sources of income) and requesting additional documentary evidence or utilizing publicly available sources (e.g. scrutiny of negative media news, internet searches, use of social media).

ii. Understand the customer's ownership and control structure to ensure that the risk associated with the relationship is well-known. This may include obtaining and assessing information regarding the customer's reputation including any negative media allegations against the customer.

[32] Regulation 14(2) and 15(5), Regulation 20(3) and Regulation 21.
[33] Section 55(2).

iii. Understand the intended nature of the business relationship and the reasons for intended or performed transactions. This may include obtaining information on the number, size and frequency of transactions that are likely to be conducted. It may be appropriate to request a customer's, business plans, cash flow projections, copies of contracts with vendors etc. The financial institution should understand why the customer is requesting a certain service or product particularly when it is unclear why the customer is seeking to establish business relationships in another jurisdiction from where he is domiciled. The account may have to be monitored for a period of time to establish a full view of the nature of activity and whether it fits with the initial risk profile of the customer.

iv. Establish the source of funds or source of wealth of the customer. Where the risk associated with the customer is particularly elevated, intrusive measures to verify the source of funds and wealth may be the only adequate risk mitigation measure. Possible sources may be reference to VAT and income tax returns, pay-slips, title deeds or, if from an inheritance, request a copy of the will or documentation to evidence divorce settlement or sale of property or other assets.

v. Evaluate the principals and conduct reference checks and checks of electronic databases;

vi. Review current financial statements; and

vii. Conduct enhanced, ongoing monitoring of the business relationship, by increasing the number and timing of controls applied, and through more frequent formal review.

The availability and use of other financial information held is important for reducing the additional costs of collecting customer due diligence information and can help increase a financial institution's understanding of the risk associated with the business relationship. Where appropriate and practical and where there are no data protection restrictions, financial institutions should take reasonable steps to ensure that where customer due diligence information is available in one part of the business, that there are information sharing mechanisms to link it to information held in another.

6.4.2 Enhanced Monitoring

The following are examples of measures a financial institution may employ to monitor high risk customers:

i. Conducting more frequent reviews of the business relationship and establishing more stringent thresholds for updating CDD information;

ii. Setting specific business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;

iii. Requiring senior management approval at the transaction level for products and services that are new for the customer;

iv. Reviewing transactions more frequently against red flag indicators relevant to the relationship. This may include establishing the purpose and destination of funds and obtaining more information on the beneficiary before conducting the transaction;

v. Flagging unusual activities and escalating concerns and transactions for senior management's attention.

7. SPECIFIC HIGHER RISKS

7.1 Politically Exposed Persons [34]

The FATF references the United Nations Convention against Corruption (UNCAC) which defines PEPs as "*individuals who are, or have been, entrusted with prominent public functions and their family members and close associates*". Individuals holding such positions may misuse their power and influence for personal gain or advantage, or for the personal gain or advantage of family members and close associates. Family and close associates may also be used to conceal misappropriated funds or assets from abuse of their position or received from bribery. PEPs may use their position to gain access to, or control of, legal entities for personal gain.

Financial institutions are required to have appropriate risk-management systems and procedures to identify when their customer (or the beneficial owner of a customer) is a PEP and to manage any elevated risks. Business relationships with the family and known close associates of a PEP should also be subject to greater scrutiny. These requirements are intended to be preventive and should not be interpreted as stigmatising all PEPs as being involved in criminal activity. The majority of PEPs are neither in a position to, nor do they abuse their official position and will therefore, not represent elevated risk solely by their categorization as a PEP.

Notwithstanding the foregoing, financial institutions must take reasonable measures to determine whether a customer is a:

i. Foreign or domestic PEP;

ii. a director or member of the board (or equivalent function) of an international organization; or

iii. An immediate family member or close associate of a PEP.

Senior management approval must be obtained for establishing or continuing business relationships with all PEPs[35]. Foreign PEPs, their immediate family members and their close associates must automatically be treated as high-risk clients and be subject to EDD measures, including reasonable measures to establish their source of wealth[36] and source of funds for the business relationship.

It is not expected that financial institutions will automatically treat domestic PEPs and PEPs associated with an international organization as high risk. Once the PEP status has been established, the financial institution must assess the customer to determine whether the relationship poses a high ML/TF risk, categorize the relationship and conduct due diligence in accordance with its risk appetite and internal policies and procedures.

Risk factors which may be considered include the political environment and the vulnerability of the PEP's country to corruption, the rationale for wishing to open an account in a jurisdiction other than where political office is held and the products or services sought by the PEP. A private

[34] Refer to definition of a PEP in Regulation 20 of the FOR
[35] Refer to Regulation 20(4) of the FOR
[36] For foreign PEPs some jurisdictions require public officials to file asset and income declarations which are publicly available. Some jurisdictions also impose restrictions on their PEPs ability to hold foreign bank accounts. The World Bank has compiled a library on the disclosure laws for various jurisdictions.

banking/wealth management relationship poses a different level of risk from having a simple banking account to facilitate domestic expenses. Similarly, a PEP with third party motor insurance presents lower risk than a PEP who has life insurance products or investment related insurance.

Where a business relationship with a PEP is not initially deemed to be high risk, it may evolve into a higher risk business relationship at a later stage. Financial institutions are therefore required to have in place appropriate ongoing monitoring systems to ensure that changes in the risk profile of such customers can be identified and enhanced due diligence applied.

Refer to Part IV of this Guideline for additional guidance and for information on the categories of PEPs as defined in the FOR and examples of lower and higher risk indicators.

7.1.1 Time Limits on PEP Status

The treatment of a customer who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits. In this regard, possible risk factors to consider are:

i. The seniority of the position that the individual held as a PEP;

ii. Whether the individual's previous and current function are linked in any way (e.g., his involvement in the appointment of his successor);

iii. Whether the PEP continues to deal with the same substantive matters and the level of influence that the individual may still exercise.

Similarly, the period for which family members and close associates of PEPs who have demitted office, should be treated as PEPs, is directly related to the assessment of risk for the primary PEP.

Financial institutions should not establish business relationships with PEPs if the financial institution knows or has reason to suspect that the funds derive from corruption or misuse of public assets. Senior management has the ultimate responsibility to ensure that the personal circumstances[37], income sources and wealth of PEPs are known and verified as far as reasonably practical.

7.2 Non Face-to-Face Business

It is important to note that not all non face-to-face business relationships will present higher risk. Examples of potentially higher risk situations include where there is no direct face-to-face communication with the customer such as during the account opening process or where products or services facilitate anonymity. Examples include conducting transfers according to instructions conveyed by customers over the internet, post, fax or telephone. Non face-to-face applications and transfers undertaken across the internet pose greater risks than other non-face-to-face business due to the following factors which collectively aggravate the ML/TF risks:

i. The ease of unauthorized access to the facility, across time zones and location;

[37] This includes information on (i.) estimated net worth, including financial statements; (ii) immediate family members or close associates having transaction authority over the account; and (iii.) references or other information to confirm the reputation of the client.

ii. The ease of making multiple fictitious applications without incurring extra cost or the risk of detection;

iii. Absence of physical documents; and

iv. The speed of electronic transfers.

The measures taken for verification of a customer's identity in respect of non-face-to-face business relations with or transfers for the customer will depend on the nature and characteristics of the product or service provided and the customer's risk profile.

Where verification of identity is performed without face-to-face contact (e.g. electronically), additional checks should be applied to manage the risk of fraud. The additional checks may rely on existing anti-fraud checks that the financial institution routinely undertakes as part of its existing procedures, such as:

i. Telephone contact with the customer at a residential or business number that can be verified independently;

ii. Confirmation of the customer's address through an exchange of correspondence or other appropriate method;

iii. Telephone confirmation of the customer's employment status with his employer's human resource department at a listed business number of the employer;

iv. Confirmation of the customer's salary details by requiring the presentation of a recent job letter or bank statement, where applicable; or

v. Provision of certified identification documents by lawyers or notaries public[38].

7.3 Non-profit organizations (NPOs)

NPOs differ in size, income, structure, legal status, membership and scope. They engage in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes or for carrying out other types of "good works". NPOs can range from large regional, national or international charities to community-based self-help groups. They also include research institutes, churches, clubs, and professional associations. They typically depend in whole or in part on charitable donations and voluntary service for support.

EDD may not be necessary for all NPO customers as not all NPOs are high risk. Many are small organizations dealing with insignificant donations for redistribution among members. The FATF has adopted a functional definition[39] of a NPO based on activities and characteristics which put it at risk of terrorist financing abuse. FATF also noted that NPOs most at risk of abuse for terrorist financing are primarily engaged in 'service activities'. These are programmes focused mainly on providing housing, social services, education or health care. Even within this sub-set of NPOs, the risk is not equal. There is a stronger risk of abuse for NPOs providing services in close proximity to an active terrorist threat such as an NPO operating:

i. In a conflict zone where there is an active terrorist threat; or

[38] Examples of suitable certifiers include a justice of the peace, notary public, police officer above the rank of sergeant and commissioners of affidavits.
[39] Interpretive Note to Recommendation 8 of the FATF Recommendations

ii. Domestically in a country where there may not be conflict but is within an area targeted by a terrorist movement for support and cover.

In this regard, it is important for financial institutions to determine the level of risk associated with the activities which the NPO engages in and make the appropriate distinction between those that serve a limited social or regional purpose from those whose activities and connections are more sophisticated, or are geographically based near to conflict zones and / or with financial links to other countries.

To assess the risk, a financial institution should consider:

i. The evidence of registration under applicable laws of the home and local operation;
ii. The purpose, ideology or philosophy of the NPO;
iii. The geographic areas served (including headquarters and operational areas);
iv. organizational structure;
v. The NPO's donor and volunteer base;
vi. Funding and disbursement criteria (including basic beneficiary information);
vii. Record keeping requirements;
viii. Affiliation with other NPOs, Governments or groups;
ix. Identity of all signatories to the account; and
x. Identity of board members and trustees, where applicable.

As part of the verification process, financial institutions should carry out due diligence against publicly available terrorist lists and monitor on an ongoing basis whether funds are being sent to high-risk countries. Where a non-profit association is registered in an overseas jurisdiction, it may be useful to contact the appropriate charity commission or equivalent body, to confirm the registered number of the charity and to obtain the name and address of the commission's correspondent for the charity concerned. Financial institutions should satisfy themselves as to the legitimacy of the organization by, for example, requesting a copy of the constitution.

Whilst it is not practical to obtain documentary evidence of identity of all donors, where possible, financial institutions should undertake a basic level of due diligence of a foreign NPO's donors in relation to known ML/TF activities.

7.4 Corporate Customers with the Ability to issue Bearer Shares

The Companies Act Chapter 81:01 prohibits the use of bearer shares, nominee shares and nominee Directors. Bearer shares can mask the identity of beneficial owners of a corporate customer with the heightened risk that the anonymous owners utilize the bearer shares or the company for ML/TF purposes.

Where a financial institution becomes aware that a new applicant or existing customer has the ability to issue bearer shares, the decision to enter or maintain the relationship should be subject to EDD measures, including reasonable effects to identify persons who beneficially own 10% or more of the corporate customer, taking into account issued or outstanding bearer shares. One or more of the following measures must also be applied:

i. Require the customer to immobilize issued and outstanding bearer shares with an approved custodian. An approved custodian must be suitable and reputable which may include on a risk basis:

- Be a regulated financial entity or well-known corporate service provider;
- Confirmation of existence;
- Subject to public source negative/adverse searches;
- Identification and verification as appropriate of the entity and all owners.

ii. Require the customer to amend the constitutional documents of the legal person (or provide other documents as appropriate in the respective jurisdiction), to remove the ability to issue bearer shares;

iii. Require the customer to convert the bearer shares to registered shares and/or evidence that all outstanding bearer shares have either been cancelled or registered.

7.5 Technological Developments

The accelerated development and increased functionality of new technologies to provide financial services create challenges for countries and private sector financial institutions in ensuring that these types of payment products and services are not misused for ML/TF purposes. Virtual currencies and various forms of electronic money, for example, are emerging as potential alternatives to traditional payment methods.

Financial institutions must assess the ML/TF risks associated with the introduction of:

i. New financial products and services and/or changes to existing products and services;

ii. New or developing technologies used to provide services.

In such instances, financial institutions must also consider as applicable, the Central Bank's Guidelines regarding new or materially different products and services[40] and whether the Central Bank should be notified.

Financial institutions must also assess the level of risk associated with potential or existing customers who offer technologically innovative products and services, such as FinTech companies, to determine whether the relationship poses higher ML/TF risk and thereafter, categorize the relationship and conduct due diligence accordingly. In this regard, financial institutions should ensure there are systems and controls in place to identify emerging ML/TF risks, assess and where appropriate, incorporate these into the risk assessments in a timely manner. Examples of systems and controls to identify emerging risks may include:

[40] For banking products and services: https://www.central-bank.org.tt/publications/legislations-and-guidelines/banking-sector-legislation-and-guidelines. For Insurance products and services: https://www.central-bank.org.tt/publications/legislations-and-guidelines/insurance-sector-legislation-and-guidelines

i. Measures to ensure internal information is reviewed regularly to identify trends and emerging issues, both in relation to individual business relationships and the financial institution's business;

ii. Regular reviews of relevant information sources; and

iii. Processes to capture and review information on risks relating to new products and services.

The Central Bank will continue to monitor developments on new payment methods and provide additional guidance as necessary on emerging best practices to address regulatory issues in respect of ML/TF risks.

8. TRANSACTION MONITORING

Financial institutions must have appropriate processes in place that allow for the identification of unusual transactions, patterns and activity that is not consistent with the customer's risk profile[41]. Since these will not all be suspicious, financial institutions should also have processes to analyse transactions, patterns and activity to determine if they are suspicious and meet the reporting threshold.

Transaction monitoring processes or systems may vary in scope or sophistication (e.g. using manual spreadsheets and exception reports to automated and complex systems or a combination of both) depending on the size, volumes and complexity of the business operations. Regardless, the key element of any system is having up-to-date customer information to facilitate the identification of unusual activity.

Monitoring can be either:

i. In real time, in that transactions and/or activities can be reviewed as they take place or are about to take place; or

ii. After the event through an independent review of the transactions and/or activities that a customer has undertaken.

Financial institutions should also have systems and procedures to deal with customers who have not had contact for some time, such as dormant accounts or relationships, to be able to identify future reactivation and unauthorized use.

In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk. Monitoring processes and systems should enable trend analysis of transaction activity including monitoring of transactions with parties in higher risk countries or jurisdictions, to identify unusual or suspicious business relationships and transactions. The monitoring system should enable financial institutions to monitor and report to senior management on significant customer relationships and activity on an individual or consolidated basis across the financial group and identify activity that is inconsistent with the financial institution's knowledge of the customer, their business and risk profile.

[41] Refer to section 6 of this Part for KYC/CDD guidance and to Part IV for guidance on conducting an ML/TF risk assessment to develop the customer's risk profile.

The parameters and thresholds used to generate alerts of unusual transactions/activity should be customized to be commensurate with a financial institution's ML/TF risk profile and the complexity and extent of its business activities. Standard parameters provided by the vendor may be used but the financial institution must be able to validate and demonstrate to the Central Bank that these are appropriate for the institution's risk position. The monitoring system should be tested on a periodic basis to ensure that the parameters are performing as expected and remain relevant. Modifications may be required as a result of such testing. Findings, analysis and the proposed modifications should be documented indicating:

i. The rationale for reviewing the parameters and thresholds;

ii. Details of testing; any assumptions made and the analysis of outcomes; and

iii. The changes made to the parameters and thresholds.

Financial institutions may refer to guidance on model validation[42] issued by the Office of the Comptroller of the Currency (OCC).

8.1 Identifying and Reporting Unusual or Suspicious Activity/ Transactions

Where the financial institution knows or has reasonable grounds to suspect that the funds or activity being placed with it represent the proceeds of criminal activity or may be related to the financing of terrorism the financial institution must file a suspicious transaction/activity report (STR) with the FIU.

Financial institutions must ensure that in the course of submitting the STR that utmost care is undertaken to ensure that such reports are treated with the highest level of confidentiality. It is an offence for employees, directors, officers or agents of a financial institution to disclose even indirectly, that a suspicious transaction report or related information on a specific transaction has been, is being, or shall be filed with the FIU. This is known as 'tipping off'[43].

Internal investigations to determine whether unusual/suspicious activities/transactions have legitimate economic or lawful purpose, where conducted properly and in good faith, are not regarded as tipping off. When a suspicious activity report is made to the FIU in good faith, financial institutions, their employees, directors, owners or other representatives are exempted legally from criminal, civil or administrative liability as the case may be, or for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, regardless of the result of the communication[44].

Initial detection or identification of unusual/suspicious activities/transactions, including attempted transactions, may occur:

i. When a transaction is flagged through an automatic alert or through a manual process or both;

ii. Through employee engagement with the customer or through a review of the customer's file and employee knowledge of the customer's business and circumstances; or

[42] Supervisory Guidance on Model Risk Management, OCC, April 2011
[43] Refer POCA 51(1).
[44] Refer POCA 55B.

iii. Third party public sources (e.g. news media, internet, credit checks, etc.).

Guidance on STR standards may be obtained from the FIU's website .

The process to determine whether the unusual activity or transaction is suspicious or whether reasonable grounds to suspect exist must be conducted *as diligently and as quickly as possible*. The determination may be made at virtually the same time of detection of the unusual activity/transaction, or the financial institution may need to conduct more comprehensive enquiries and examination of past and related account activity. As soon as a financial institution determines that the threshold for suspicion or reasonable grounds for suspicion has been met and that the funds are the proceeds of criminal activity or related to TF, a STR must be immediately filed with the FIU.

Where there are common customers within a financial group context, consideration of the risk exposure must be made and as far as possible, information on the customer or transaction must be shared to ensure that all facts are considered and consistent decisions are made group-wide. Such instances must be immediately brought to the attention of the GCO.

Financial institutions are required to maintain comprehensive records[45] of the review and adjudication process for investigating unusual/suspicious activity/transactions, including monitoring alerts determined to be 'false positives' or where a determination has been made to close an alert or an internal suspicious activity report and not report it to the FIU.

8.2 Monitoring and Reporting Mechanisms

Financial institutions must develop systems and procedures to assist in the identification of unusual or suspicious activity in all types of business transactions, products and services offered, and particularly for transactions with high risk customers such as PEPs and use of high risk services such as wire transfers and private banking. To facilitate the detection of suspicious activity/transactions, a financial institution should:

i. Require customers to indicate/reveal the source and/or purpose of funds for business transactions in excess of threshold limits, or such lower amount (i.e. wire transfers) as the financial institution determines, to ascertain the legitimacy of the funds;

ii. Develop written policies, procedures and processes to provide guidance on unusual/suspicious criteria or 'red flags' and on the reporting procedures to follow when identifying, investigating and reporting unusual activity/transactions; and

iii. Require its employees to document in writing their suspicion about a transaction.

Financial institutions may refer to Part V of this Guideline which provides examples of transactions and activities, including fraud indicators that may be triggers or red flags for the purpose of reporting suspicious activity and transactions to the FIU. These are not intended to be exhaustive and are only examples of the most basic ways in which money may be laundered or used for TF purposes.

[45] May be either electronic and/or physical records

8.3 Internal Reporting Procedures

Financial institutions must ensure that there are internal processes and procedures for employees to identify and report unusual activities/transactions to the designated CO and for maintaining employee awareness of indicators of potential suspicious activities/transactions.

All employees must be made aware:

i. Of the identity of the designated CO and that his identity is to remain confidential;

ii. That all unusual/suspicious activity/transactions must be reported as soon as reasonably practicable to the CO, after the activity/transaction has been observed and that such reports are to remain confidential;

iii. Of the procedure to be followed when making a suspicious activity report; and

iv. That where suspicious activities continue on an account which they have previously reported to the CO, they must continue to make reports to the CO whenever additional suspicious transactions occur.

All such reports must be submitted to the CO who has the ultimate authority to determine whether a disclosure to the FIU in accordance with the legislation is appropriate. Some financial institutions may have internal reporting procedures that allow an internal suspicious activity report (iSAR) to be channeled through the relationship or line manager before submission to the CO. Where such internal reporting procedures are in place, those officers cannot alter the report but may attach their comments as to why they believe that the suspicion is not justified. Regardless, all reports of suspicious activities must be submitted to the CO.

8.4 Ongoing Monitoring of Relationships

Once suspicion has been raised regarding a customer relationship or transaction, in addition to filing the STR with the FIU, the financial institution must ensure that appropriate measures are put in place to mitigate the risk that the financial institution is used for criminal activity. Such measures may include:

i. Review of the customer account/relationship and the risk classification and undertaking additional due diligence;

ii. Enhanced monitoring of the relationship/transactions;

iii. Imposition of restrictions on the customer relationship; or

iv. Escalation to the relevant senior officers to determine how to handle the relationship going forward and whether to terminate the customer relationship.

8.5 Reporting Declined Business

It is normal practice for financial institutions to turn away business that they suspect might be criminal in intent or origin. Where an applicant for business or a customer fails to provide adequate documentation, including the identity of any beneficial owners or controllers, in addition to declining the business, consideration should be given to filing a SAR.

Where an attempted transaction gives rise to knowledge or suspicion of money laundering or terrorist financing, that attempted transaction should be reported to the FIU. Reporting of such events will allow the FIU to build a clearer picture of the money laundering threat, and to use such intelligence on a proactive basis. Furthermore, the financial institution should refrain from referring such business to other financial institutions.

9. IDENTIFICATION OF DESIGNATED ENTITIES AND PERSONS & FREEZING OF FUNDS

Financial institutions must be able to identify and to comply with reporting and freezing instructions issued by the FIU regarding individuals and entities designated by the United Nations Security Council or by the High Court as terrorist entities. Notices issued by the FIU in this regard and the consolidated list may be accessed at the FIU's website.

Pursuant to Section 22AB of the ATA, financial institutions have specific obligations to immediately report to the FIU where any of the following apply:

i. A person or entity named on the UN or consolidated lists has funds in the financial institution;

ii. The financial institution has reasonable grounds to believe that the designated person or entity has funds in Trinidad and Tobago; and

iii. If the designated person or entity attempts to enter into a transaction or continue a business relationship, a suspicious transaction/activity report must be submitted immediately to the FIU. The financial institution must not enter into or continue such transaction with the designated person or entity. Funds already deposited with or held by the financial institution must remain frozen subject to any exception in the Order of the High Court.

It should be noted that the consolidated lists set out all Orders issued by the High Court under Section 22B (3), which may include an Order to immediately freeze the funds of the listed entity. In such a case, where the financial institution identifies funds of a listed person in Trinidad and Tobago, the financial institution should treat such funds as frozen pursuant to the Order of the High Court.

Terrorist screening is not a risk-sensitive due diligence measure and must be carried out regardless of the customer risk profile. Financial institutions must have processes in place to screen customer details and payment instructions against the designated lists of persons and entities and to ensure that the lists being screened against are up to date. Screening measures should consider:

i. Continuous risk based screening of customer records;

ii. Immediate screening of one-off, occasional transactions before the transaction is completed;

iii. Procedures to screen applicable payment messages; and

iv. Procedures to screen payment details on wire transfers and remittances to reasonably ensure that originator, intermediary and beneficiary details[46] are included on the transfers.

Financial institution's policies and procedures should address:

i. The information sources used by the financial institution for screening (including commercial databases used to identify designated individuals and entities);

ii. The roles and responsibilities of the financial institution's employees and officers involved in the screening, reviewing and dismissing of alerts, maintaining and updating of the various screening databases and escalating potential matches;

iii. The frequency of review of such policies, procedures and controls;

iv. The frequency of periodic screening;

v. How potential matches from screening are to be resolved by the financial institution's employees and officers, including the process for determining that an apparent match is a positive hit and for dismissing a potential match as a false match; and

vi. The steps to be taken by the CO for escalating potential or positive matches to senior management and reporting potential or positive matches the FIU.

9.1 Trade/Economic Sanctions

Economic and trade sanctions are imposed against countries, governments, entities and persons with a view to bringing about changes in policies and behavior. Governments typically impose economic sanctions to give effect to decisions made by international organizations such as the United Nations or individual or groups of countries such as the United States, Canada or the European Union. These may take the form of:

i. Prohibitions against providing financial services;

ii. Travel bans;

iii. Embargoes on arms and military products; and

iv. Prohibitions or control of trade involving certain markets, services and goods.

Financial institutions should be aware of such sanctions and consider whether these affect their operations and any implications to the financial institution's policies and procedures particularly with respect to international transfers and its correspondent relationships. In addition to screening payment instructions to identify designated terrorists, financial institutions should also screen or filter payment instructions prior to their execution in order to prevent making funds available in breach of sanctions, embargoes or other measures.

[46] Refer to Regulations 34 and 35 of the FOR

10. KNOWING YOUR EMPLOYEE (KYE)

In addition to knowing the customer, a financial institution must have robust procedures in place for knowing its employees. In this regard, every financial institution should have a recruitment policy to attract and retain employees of the highest levels of integrity and competence[47]. The ability to implement an effective AML/ CFT programme depends in part on the quality and integrity of employees.

Consequently, financial institutions should undertake due diligence on prospective employees and throughout the course of employment. At a minimum, the financial institution should:

i. Verify the applicant's identity and personal information including employment history and background. Consider credit history checks on a risk-based approach;

ii. Develop a risk-focused approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, education and professional qualifications;

iii. Maintain an ongoing approach to screening for specific positions, as circumstances change, or for a comprehensive review of employees over a period of time. Internal policies and procedures should be in place (e.g. codes for conduct, ethics, conflicts of interest) for assessing employees;

iv. Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided.

Verification should generally include the following:

i. Reference checks

ii. Checking the authenticity of academic qualifications

iii. Verifying Employment History

The names, addresses, position titles and other official information pertaining to employees appointed or recruited by the financial institution should be maintained for up to a period of six years after termination of employment and made available to the Central Bank upon request.

Financial institutions should ensure to the extent permitted by the laws of the relevant country, that similar recruitment policies are followed by its branches, subsidiaries and associate companies abroad, especially in those countries which are not sufficiently compliant with the recommendations of the Financial Action Task Force[48].

[47] Refer to Regulation of the FOR
[48] Refer to Regulation 5(3) of the FOR

In addition, to a robust recruitment policy, financial institutions should implement ongoing monitoring of employees to ensure that they continue to meet the institution's standards of integrity and competence.

Financial institutions should establish and maintain procedures to ensure high standards of integrity among employees, including the meeting of statutory "fit and proper" criteria of the officers of the company. Integrity standards should be documented and accessible to all employees. These procedures may include standards for:

i. acceptance of gifts from clients;
ii. social liaisons with clients;
iii. disclosure of information about clients who may be engaged in criminal activity;
iv. confidentiality;
v. detection of any unusual growth in employees' wealth; and
vi. deterring employees from engaging in illegal activities that can be detected by reference to his investment records.

The standards should include a code of ethics for the conduct of all employees and procedures should allow for regular reviews of employees' performance and their compliance with established rules and standards. It should also provide for disciplinary action in the event of breaches of these rules.

Financial institutions should monitor employees paying particular attention to employees whose lifestyles cannot be supported by their salary or known financial circumstances. Supervisors and managers should be encouraged to know the employees in their department and investigate any substantial changes in their lifestyles which do not match their financial condition. Procedures should provide for special investigation of employees who are associated with unexplained shortages of funds.

11. TRAINING AND AWARENESS PROGRAMME

An integral element of the fight against money laundering and the financing of terrorism is the awareness of those charged with the responsibility of identifying and analyzing potential illicit transactions. Therefore, in accordance with Regulation 6 of the FOR, financial institutions are required to ensure that appropriate training is conducted with directors and all relevant employees (on an ongoing basis) to equip them to perform their obligations in respect of AML/ CFT requirements.

Financial institutions should conduct AML/CFT training for all new directors and relevant employees and should at least on an annual basis conduct refresher training programmes to ensure that employees remain familiar with and are updated in regards to their responsibilities. Refresher programmes should address among other things new AML/CFT typologies, legislative updates (including new and proposed amendments) and international developments in AML/CFT.

At a minimum, a financial institution is required to:

i. Develop an appropriately tailored training and awareness programme consistent with the financial institution's size, resources and type of operation to enable relevant

employees to be aware of the risks associated with ML and TF. The training should also ensure employees understand how the institution might be used for ML or TF; enable them to recognize and handle potential ML or TF transactions; and to be aware of new techniques and trends in money laundering and terrorist financing;

ii. Document, as part of their AML/ CFT policy document, their approach to training, including the frequency, delivery channels and content;

iii. Ensure that all employees are aware of the identity and responsibilities of the CO to whom they should report unusual or suspicious transactions;

iv. Establish and maintain a regular schedule of new and refresher programmes, appropriate to their risk profile, for the different types of training required for:

- new employees;
- operations employees;
- agents
- supervisors;
- board and senior management; and
- audit and compliance employees.

v. Obtain an acknowledgement from each employees on the training received;

vi. Assess the effectiveness of training; and

vii. Provide all relevant employees with reference manuals/materials that outline their responsibilities and the institution's policies. These should complement rather than replace formal training programmes.

Training should be targeted to all relevant employees but the scope and frequency of training should be tailored to the specific risks faced by the financial institution and to the nature of their responsibilities. New employees and officers should be required to attend training as soon as possible after being hired or appointed. Emphasis should be placed on the continuous training of the CO as well as the compliance and audit employees given their critical role in sensitizing the broader employees complement to AML/CFT issues and ensuring compliance with established AML/ CFT policies and procedures.

A financial institution should clearly explain to its directors, senior management and employees the laws, the penalties for non-compliance, their obligations and the requirements concerning customer due diligence and suspicious activity reporting. In particular directors, senior management and other employees should be sensitized as to:

i. The importance of adhering to customer due diligence policies, the processes for verifying customer identification and the circumstances for implementing enhanced due diligence procedures;

ii. The procedures to follow for detection of unusual or suspicious activity across lines of business and across the financial group;

iii. The completion of unusual and suspicious transaction reports; Treatment of incomplete or declined transactions; and

iv. The procedures to follow when working with law enforcement or the FIU on an investigation.

The effectiveness of the institution's training programme may be assessed by:

i. Testing employees' understanding of the policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognize suspicious transactions; and

ii. Monitoring the compliance of employees with the AML/CFT procedures as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken.

Financial institutions are also required to maintain records of employee training which at a minimum should include:

i. Details of the content of the training programmes provided;

ii. The names of employees who have received the training;

iii. The date on which the training was delivered;

iv. The results of any testing carried out to measure employees understanding of the anti-money laundering requirements; and

v. An on-going training plan.

12. RECORD KEEPING PROCEDURES

Maintaining complete and updated CDD records is essential for financial institutions to adequately monitor customer relationships, to understand customers' ongoing business and activities and, for assisting with criminal investigations. Financial institutions should establish a document retention policy that provides for the maintenance of a broad spectrum of records, including those related to customer identification, business transactions, internal and external reporting and training. Once a business relationship has been formed, the financial institution should maintain records of client identification and transactions performed[49].

The document retention policy should incorporate the requirement that a financial institution is required to keep records of all domestic and international transactions as well as identification data on a customer for a minimum period of six (6) years[50], unless a longer time period is required by other statutory requirements or mandated by the Central Bank. It may also be necessary for financial institutions to retain records, until such time as advised by the FIU or the High Court, for a period exceeding the date of termination of the last business transaction where there:

i. Has been a report of a suspicious activity; or

[49] Refer to Regulations 32, 33 and 34.
[50] For one-off transactions, for relationships which have ended and for existing customers.

ii. Is an on-going investigation relating to a transaction or client.

Records should be retained in a format, including physical, electronic, scanned or microfilm, that would facilitate reconstruction of individual transactions (including the amounts and types of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity and to enable financial institutions to comply swiftly with information requests from the FIU or from Law Enforcement Agencies[51]. This applies whether or not records are stored off the premises of the financial institution.

Financial institutions should ensure that records held by a subsidiary or affiliate outside Trinidad and Tobago at a minimum, comply with the requirements of Trinidad and Tobago's laws and this Guideline.

Where the financial institution has outsourced any or all of the foregoing functions to a company in another jurisdiction then it must be satisfied that the relevant records will be maintained in accordance with Trinidad and Tobago's laws and will be available to the Central Bank and to the FIU or law enforcement authorities on request.

When a financial institution either merges with or acquires another financial entity, it should ensure that the records such as customer due diligence, transactions, external audit and training can be readily retrieved. Where the records are kept in a contractual relationship by an entity other than a financial institution, the financial institution is responsible for retrieving those records before the end of the contractual arrangement.

Each financial institution is required to maintain a register of all enquiries and containing such details as specified in Regulation 38 of the FOR.

[51] Regulation 32 of the FOR

PART III

CONDUCTING THE ML/TF RISK ASSESSMENT

Part III – Conducting the ML/TF Risk Assessment

The guidance in this Part is designed to assist financial institutions with conducting an ML/TF risk assessment[52]. A risk assessment is the first step financial institutions must take in developing an AML/CFT programme. It involves identifying and assessing the risks the business reasonably expects to face from ML/TF. Once a risk assessment is completed, financial institutions can then put in place a programme that minimises or mitigates these risks.

It is not mandatory to adopt the process this guideline sets out for preparing a risk assessment. As long as a financial entity complies with its regulatory AML/CFT obligations, it can choose a risk assessment method that best suits its business.

1. Sources of Information for the Risk Assessment

When conducting or updating risk assessments, financial institutions should consider information obtained from relevant internal and external sources, such as:

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

ii. Internal/external audit and regulatory findings;

iii. Sectoral emerging risks and typologies;

iv. Corruption indices and country risk reports;

v. Guidance issued by regulators;

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

vii. National risk assessment reports;

viii. Independent and public assessment of a country's or jurisdiction's overall AML/CFT 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 FSRBs public statements.

2. ML/TF Risk Assessments

There is no single prescribed or universally accepted methodology for conducting an AML/CFT risk assessment. A risk assessment should consist of two distinct but related steps:

i. Identification of ML/TF risk, and

ii. Assessment of the ML/TF risk and the likelihood that the financial institution will be used for ML/TF.

The steps taken to identify and assess ML/TF risk must be proportionate to the nature, size and complexity of the financial institution. Financial institutions that do not offer complex products or services and have limited or no international exposure may not need an overly sophisticated risk assessment. However, where products and services offered by the financial institution are more

[52] Pursuant to Regulation 7(2) of the Financial Obligations Regulations, 2010 (as amended)

varied and where there are multiple subsidiaries and different business units catering to a more diverse customer base through multiple delivery channels, the financial institution should conduct a more comprehensive risk assessment and identify and assess ML/TF risks on a group-wide level across all its business units, product lines and delivery channels.

In conducting the risk assessment to identify those areas of its business that may be susceptible to ML/TF risk, the financial institution should consider the following risk factors where applicable:

i. In relation to customers:

- Target customer markets and segments;
- Profile and number of customers identified as higher risk;
- Complexity, volume and size of its 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 PEP; whether the customer's employment income supports account activity).

ii. In relation to the countries or jurisdictions the financial institution is exposed to, either through its cross border and international operations or through the activities of its customers, including the financial institution's correspondent relationships:

- The AML/CFT laws, regulations and standards of the country or jurisdiction and quality and effectiveness of implementation of the AML/CFT regime;
- Contextual factors such as political stability, maturity and sophistication of the regulatory and supervisory regime, level of corruption, financial inclusion etc.

iii. In relation to the products, services, transfers and delivery channels of the financial institution:

- Nature, scale, diversity and complexity of the financial institution's business activities including its geographical diversity;
- Nature of products and services offered by the financial institution;
- 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;
- the degree to which the operations are outsourced to other entities in the Group or third parties; and
- 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.

3. CUSTOMER RISK ASSESSMENT

Financial institutions should also consider the nature and level of risk posed by a customer to determine the applicable due diligence. Policies and procedures should facilitate collection of information to develop risk profiles, either for specific customers or categories of customers. Customer risk profiles facilitate the identification of any account activity that deviates from 'normal' activity or behaviour which may be considered unusual or even suspicious. Risk profiles also assist with determining if the customer or customer category is higher risk and require the application of enhanced customer due diligence measures and controls. In developing customer risk profiles, the financial institution should consider:

i. The nature and purpose of the customer relationship; the anticipated volumes and transactional activity; and the source of origin and destination of funds;

ii. Who the customer is and whether he falls into higher categories of risk, for example, a PEP, a high net worth client, or is a correspondent bank;

iii. The product and services accessed by the customer and those that pose higher risk such as wire transfers or private banking services;

iv. The customer's business location and the location of his counterparties and any associated geographic risk, including understanding why the customer chose to open an account outside of its domiciled location or jurisdiction.

While a risk assessment should always be performed at the start of the customer relationship, for some customers a comprehensive risk profile may only become evident after the customer begins transacting through an account. Consequently, having a system in place to monitor customers' transactions on an on-going basis is a fundamental component of a risk based AML/CFT compliance programme.

Part V of this Guideline illustrates sector specific risk factors a financial institution may consider when assessing the ML/TF risk posed by customer situations.

4. ASSESSING THE LIKELIHOOD OF THE FINANCIAL INSTITUTION BEING USED FOR ML/TF

Financial institutions should take a holistic view of the ML/TF risk factors they have identified to determine the level of ML/TF risks associated with a business relationship or occasional transactions. As part of this assessment, financial institutions may decide to weigh factors differently depending on their relative importance and within the context of the business relationship or an occasional transaction. For example, a customer from a high risk jurisdiction may be less relevant if the banking account is solely to facilitate the receipt of salary and payment of household expenses and is not used for the receipt and international transfer of additional funds. Similarly, the risk associated with a PEP conducting a transaction to acquire motor vehicle insurance may be lower when than a PEP purchasing life insurance or an annuity.

When weighting risk factors financial institutions should ensure that:

i. The weighting is not unduly influenced by any one factor or leads to a situation where it is impossible for business relationships to be classified as high risk;

ii. Economic or profit considerations do not influence the risk rating. As such, situations identified by AML/CFT legislation, regulations and Guidelines as presenting high ML/TF risk cannot be over-ruled by the financial institution's weighting; and

iii. Automatically generated risk scores are reviewed and over-ridden where necessary. The rationale for the decision to override such scores should be documented.

Where a financial institution does not develop its risk assessment system in-house but purchases it from an external provider, it must understand how the system works and how risk factors are assessed to achieve the overall risk score. The financial institution must be satisfied that the weightings allocated is an appropriate reflection of the ML/TF risk present in its business and it must be able to demonstrate this to the Central Bank.

5. CATEGORIZING OF ML/TF RISKS

Financial institutions may determine the most appropriate way to categorize risk, based on the nature and size of the business and the types of ML/TF risk identified from the risk assessment. Typically, ratings of high, medium and low are used but other categorizations may be applied by financial institutions at their own discretion. The criteria used for rating and ranking risks should however, have a rational basis and address ML and TF risk factors that are unique to specific business lines, customer segments, jurisdictions or any other more general risk factors. An example of a risk assessment tool is provided in the section below.

At a minimum, the risk rating framework should include:

i. Segregation of client relationships by risk categories (e.g. high, moderate or low);

ii. Differentiation of business relationships by risk factors (such as products, client type/profession, country of domicile, complexity of ownership and legal structure, source of business, type of assets, size and volume of transactions, type of transactions, cash transactions, adherence to client activity profile);

iii. The applicable know your customer (KYC) documentation and due diligence information requirements for each risk category and risk factor; and

iv. A process for the approval of the downgrading/ upgrading of risk ratings.

The risk rating framework should provide for the periodic review of the business relationship to allow the institution to determine whether any adjustment should be made to the risk rating. **The review of the risk rating for high risk customers must be undertaken more frequently than for other customers**, and where appropriate, a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

6. RISK ASSESSMENT TEMPLATE[53]

This template is not intended as a substitute for the requirement for a financial institution to determine the most appropriate way to categorize and weigh ML/TF risks[54]. Financial institutions are expected to

[53] Adapted from the Investment Management Association of Singapore

[54] Please note that this template is intended as an example to provide general guidance to assessing ML/FT risk. It is not meant to be mandatory nor definitive. The Central Bank neither approves nor disapproves use of this template. Any

perform their own due diligence in determining the most appropriate methodology for conducting the assessment. Financial institutions may choose to adjust the template according to their own specific circumstances.

6.1 Risk Assessment Instructions and Example

To conduct the risk assessment, assess your financial institution's overall risk score against the various factors listed in Annexes 1 and 2. Adjust the risk weight according to your institution's specific context, and enter the individual scores in the template to arrive at the overall risk assessment score. (Refer to the example below on how to carry out the risk assessment)

i. Assign a risk score (e.g. 1-Lower risk, 5-Higher Risk) to each individual factor based on its relative importance in identification of ML/TF risks.

ii. Each risk score is then weighted according to the level of risk exposure by the institution based on the individual factors. A weighted summation of the risk scores gives an overview of the risk exposure of the institution. Refer to Annexes 2 and 3 for possible approaches and considerations in deriving the risk scores.

Financial institutions may allocate risk weightings as deemed to be appropriate to their business context. Note that the summation of the risk weights must be 100%. In this example, risk weights of 20%, 40%, 30% and 10% respectively has been allocated to:

i. ML/TF Risk Internal Governance Framework;

ii. ML/TF Risk Factor Assessment;

iii. ML/TF Risk Mitigation Assessment; and

iv. ML/TF Training and Coordination.

The risk scores were obtained from the questionnaires in Annex 1 and Annex 2 and then imputed under the 'risk score' column of the template. The 'weighted risk score' was then obtained by multiplying the risk weight and the risk score.

a) Risk Assessment Score:

1.0 – 2.0 = ML/TF risk on a group-wide basis is low

2.0 – 3.0 = ML/ TF risk on a group-wide basis is moderate

>3.0 = ML/ TF risk on a group-wide basis is high

b) Results of Assessment:

A summation of the numbers indicates a Risk Assessment Score of **2.23.** Utilizing the risk ranges in (a) above, the financial institution's group-wide ML/ TF risk is assessed to be **moderate**.

representation to the contrary is false. The template is being provided strictly as an illustration and the Central Bank makes no undertaking, representation or statement as to the accuracy, suitability and specificity for any financial institution.

Risk Assessment Example –
Deriving the ML/TF Risk Score

Risk Factors	Risk Weight	Risk Score	Weighted Risk Score
I. ML/TF Risk Internal Governance Framework[55]	**20%**		
I.1 Compliance programme	3%	2	0.06
I.2 Board and Management support	8%	2	0.16
I.3 Documentary process	3%	3	0.09
I.4 Risk assessment conduct	3%	4	0.12
I.5 Frequency of assessment	3%	3	0.09
II. ML/TF Risk Factor Assessment[56]	**40%**		
II.1 Client risk	10%	2.3	0.23
II.2 Country risk	10%	2.19	0.22
II.3 Products, services and delivery channels	5%	2.41	0.12
II.4 Higher risk business activities	15%	2	0.3
III. ML/TF Risk Mitigation Assessment[57]	**30%**		
III.1 Vulnerabilities to ML/TF risks	6%	1	0.06
III.2 Appropriate EDD process	5%	2	0.1
III.3 Customers' risk mitigation assessment	4%	2	0.08
III.4 Customer transaction assessment	5%	3	0.15
III.5 Customer screening procedures	5%	3	0.15
III.6 Business activities review	2%	4	0.08
III.7 Periodic ML/TF audits	3%	2	0.06
IV. ML/TF Training and Coordination[58]	**10%**		
IV.1 Communication of new regulations	4%	1	0.04
IV.2 Employees training	6%	2	0.12
Risk Assessment Score	**100%**	**5**	**2.23**

[55] Refer to Annex 1: Section I
[56] Refer to Annex 1: Section II
[57] Refer to Annex 1: Section III
[58] Refer to Annex 1: Section IV

ANNEX 1 – MONEY LAUNDERING / TERRORIST FINANCING RISK ASSESSMENT

I. *ML/TF Risk Internal Governance Framework Assessment*	Yes	No	Risk Score	Comments
1. Does the financial institution have a legal and regulatory compliance programme that includes a designated officer that is responsible for coordinating, overseeing, reviewing and updating the firm's ML/TF risk assessment framework conducted on a group-wide level covering all business units, product lines and delivery channels?	√ Refer to Annex 3.1. for details		2	
2. Does the financial institution's senior management and Board approve its group-wide ML/TF risk assessment, be apprised of the assessment results and provide full support and adequate resources towards mitigating potential ML/TF risks?	√ Refer to Annex 3.2 for details		2	
3. Does the financial institution have a documentary process evidencing: • the conduct of ML/TF risk assessment; • implementation of systems and procedures to address the deficiencies identified; and • the management reporting and escalation of such matters to senior management and the Board? Does the financial institution have a process to retain records of and make them available to the Authority upon request? • What is the institution's retention period for record keeping for AML documents? • Does the retention period comply with the local regulatory requirement and group policy?	√		3	
4. Does the conduct of ML/TF risk assessment allow the financial institution to better understand its overall vulnerability to ML/TF risks and form the basis of its overall risk-based approach?	√		4	
5. Will the financial institution conduct a group-wide ML/TF risk assessment at least once in two years or when material trigger events occur, whichever is earlier? Material trigger events include but are not limited to the acquisition of new customer segments or delivery channels or the launch of new products or services.	√		3	

II. *ML/TF Risk Factors Assessment*	Yes	No	Risk Score	Comments
1. Does the financial institution consider ML/TF risk factors concerning its customers across its business units, product lines and delivery channels (in and outside Trinidad and Tobago), such as: • Target customer markets and segments; • Profile of existing customers (client segments broken down by number, country of domicile, and AML risk profile); and • Volume and size of its transactions and fund transfers, considering the usual activity and risk profile of its customers.	√ Refer to Annex 2.I and Annex 3.3 for details		2.30	
2. In relation to its own business activities and the customers assessed in II.1., does the financial institution consider ML/TF risk factors of countries or jurisdictions where there is relatively higher levels of corruption, organized crime or inadequate anti-money laundering and countering of financing of terrorism measures ("AML/CFT")?	√ Refer to Annex 2.II and Annex 3.4 for details		2.19	
3. In relation to its products, services, transactions and delivery channels, does the financial institution consider the following attributes: • Nature, scale, diversity and complexity of its business activities; • Nature of products and services offered and • Nature of delivery channels utilised? Does the financial institution also consider the following factors: • Whether reliance is placed on Customer Due Diligence (CDD) conducted by third parties. If so, what are the checks in place? • What payment processes are utilised? Are payments made to third parties? • Do products, services and delivery channels facilitate anonymity?	√ Refer to Annex 2.III and Annex 3.5 for details		2.41	
4. Does the financial institution have business relationships with the following persons or entities identified as potentially presenting higher ML/TF risks: • Shell banks or shell companies; • Persons or private legal entities controlled or influenced by Politically Exposed Persons, their family and close associates, or		√	2	

II. *ML/TF Risk Factors Assessment*	Yes	No	Risk Score	Comments
state-owned entities; • Entities that provide correspondent account services; and • Politically Exposed Persons?				

III. *ML/TF Risk Mitigation Assessment*	Yes	No	Risk Score	Comments
1. Does the financial institution take into consideration the vulnerabilities to ML/TF risks faced, into assessment and whether there are any risk mitigation approaches?	√		1	
2. Does the financial institution determine the appropriate level of enhanced due diligence necessary for categories of customers it has reason(s) to believe pose a heightened risk of conducting illicit activities?	√		2	
3. Does the financial institution assess its customer's ML/TF risk mitigation policies or practices, where relevant?	√		2	
4. Does the financial institution complete a risk-based assessment to understand the normal and expected transactions of its customers?	√		3	
5. Does the financial institution screen customers against a list of persons, entities and countries issued by governments and competent authorities and against known databases for derogatory information or association to identify changes in customer profile?	√		3	
6. Does the financial institution conduct a review to assess if existing and new business activities, products and delivery channels would be susceptible to potential abuse and prevailing crime types? • Have there been any significant changes in the business model or client profile impacting the AML/CFT activities?	√		4	
7. Is the financial institution subject to periodical internal audits and annual statutory audits which cover its adherence with regulatory requirements as part of audit scope?	√		2	

IV. *Group-wide AML/CFT Training and Coordination Assessment*	Yes	No	Risk Score	Comments
1. Does the financial institution communicate new AML/CFT laws and regulations and their changes, and updates to internal policies or practices to employees?	√		1	
2. Does the financial institution provide AML/CFT training to its employees that includes, amongst others, the following: • Specific AML/CFT regulatory requirements; • Internal policies and procedures on AML/CFT; • Examples of different forms of ML/TF and real case-studies; and • Identification of ML/FT red flags and reporting of transactions to the FIU? • Do all employees undertake AML Training? • How often is the training provided? • Is there a testing component? • Do all employees receive the same training? • If no, describe the differences in training e.g. frequency of training, level of training.	√		2	

ANNEX 2- RISK SCORING[59]

Annex 2.I Client Risk Assessment for Different Client Types

Risk Level	Risk Score	No. of clients (Retail)	No. of clients (Institutional)	Total No. of Clients	Score[60]	Average Score[61]
Higher Risk	5	5	1	6	30	
High Risk	4	10	2	12	48	
Medium Risk	3	20	3	23	69	
Low Risk	2	25	3	28	56	
Lower Risk	1	30	4	34	34	
Total		**90**	**13**	**103**	**237**	**2.30**

Annex 2.II Client-Country Risk Assessment

Risk Level	Risk Score	No. of clients in Country 1	No. of clients in Country 2	Total No. of Clients	Score	Average Score
Higher Risk	5	5	2	7	35	
High Risk	4	10	4	14	56	
Medium Risk	3	20	6	26	78	
Low Risk	2	30	8	38	76	
Lower Risk	1	40	10	50	50	
Total		**105**	**30**	**135**	**295**	**2.19**

Annex 2.III Client-Product-Channel Risk Assessment

	Risk Score	No. of clients in Channel 1	No. of clients in Channel 2	Total No. of Clients	Score	Average Score
Higher Risk	5	10	30	40	200	
High Risk	4	15	50	65	260	
Medium Risk	3	20	70	90	270	
Low Risk	2	25	90	115	230	
Lower Risk	1	30	120	150	150	
Total		**100**	**360**	**460**	**1110**	**2.41**

[59] Refer to Annex 3.II - 'Additional Considerations – ML/TF Risk Factors Assessment' when considering the appropriate risk score for the assessment.
[60] 'Score' = 'Risk Score multiplied by 'Total Number of Clients'
[61] 'Average Score' = 'Score' divided by 'Total Number of Clients'

ANNEX 3 – ADDITIONAL CONSIDERATIONS

Financial institutions may consider the following guidance in completing the risk assessment in Annex 1:

3.1. Compliance Function

In completing question one in Section I. of the ML/TF Internal Governance Framework Risk Assessment financial institutions may give consideration to the following:

a) What is the structure of AML/CFT management and how are AML responsibilities allocated within the organization?
b) Is there a designated CO who is tasked with reporting to senior management and the board of directors? If yes:
    i. *Consider their suitability to fulfil the role e.g. training, qualifications, experience, previous roles.*
    ii. *Is the CO the focal point for the oversight of all activities relating to the prevention and detection of ML/TF?*
    iii. *Is the CO independent of all operational and business functions; as far as practicable within any constraint of the size of the financial institution?*
    iv. *Is the CO of a sufficient level of seniority and authority within the institution?*
    v. *Is the CO provided with regular contact with and direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and the measures against the risks of ML/TF is sufficient and robust?*
    vi. *How conversant is the CO in the local statutory and regulatory requirements and ML/TF risks?*
c) In order to effectively manage business/operational unit's ML/TF risks, are there:
    i. *Sufficient employees?*
    ii. *Fully competent employees?*
    iii. *Adequate systems?* If not, describe the impact of this and how it is intended to manage this situation.
    iv. *Are there are plans to adopt other technology-based or automated solutions for AML/CFT risk management purposes?* If yes, please elaborate.
    v. *What is the current approach with regards to coordination with other control functions within the financial institution in relation to AML/CFT?*
d) Is it anticipated that there will be any circumstances which may have a negative impact upon the resource capability over the next 12 months?
e) In terms of the Compliance Program:
    i. *Does it adequately address all regulatory requirements, i.e. legislation, regulations and guidelines?*
    ii. *Is it reviewed, updated and approved by the Board on a regular basis?*
    iii. *Is it effectively communicated and applied throughout the financial institution?*

f) Are there processes in places to ensure effective coordination with regulatory and law enforcement agencies?

g) In relation to CDD:

i. *Is the appropriate level of due diligence undertaken for all clients in accordance with their risk profile?*

ii. *Are high risk clients subjected to appropriate on-boarding and monitoring controls?*

iii. *Do record-keeping procedures comply with the AML/CFT legislative requirements?*

iv. *Is CDD information readily available to the CO?*

v. *Does CDD testing include performance of CDD by third parties?*

vi. *How often is it conducted?*

vii. *Is the required supporting documentation governing the arrangement in place?*

viii. *Can the third party provide requested CDD information and copies of the relevant documentation immediately upon request?*

ix. *Does the third party have measures in place for record-keeping in accordance with the requirements of the AML/CFT legislation?*

h) In terms of screening of client relationships against all applicable lists including domestic lists, are there processes to*:*

i. *Screen customers conducting one-off transactions?*

ii. *Screen new client relationships?*

iii. *Screen all existing client relationships regularly to identify if they become a PEP?*

iv. *Assess whether the frequency of the client screening remains appropriate?*

v. *Require approval from higher management for newly identified PEP/ high risk client relationships?*

vi. *Identify where PEP / high risk client approvals are still outstanding?*

vii. *Ensure that positive matches are reported in accordance with regulatory requirements and appropriate action taken?*

i) In respect of suspicious activity reporting:

i. *Are procedures clear for employees to report suspicions internally?*

ii. *Are there adequate systems to monitor the suspicious activity?*

iii. *Have all employees been made aware of their personal obligations regarding the reporting of suspicious transactions?*

iv. *Are there procedures in place to ensure that suspicious activity reports are submitted in accordance with regulatory requirements (comprehensive and accurate information is provided and filed in a timely manner)?*

v. *Decisions regarding reporting or closing of suspicious activity/transaction alerts are clearly and comprehensively documented?*

j) In terms of testing and review (both Compliance and independent review) of the AML/CFT control processes, is there:

i. *A comprehensive monitoring and testing program to assess the effectiveness of the Compliance Unit and the Compliance Program?*

ii. *An assessment of business units' adherence to AML/CFT policies and procedures?*

iii. *Regular review of key AML/CFT indicators by the CO and by business units?*

iv. *A process to ensure that the Compliance Program is assessed and reported on in line with statutory requirements?*

3.2. Management Support

When completing question two in Section I, to assess the capability and responsibility of senior management in terms of AML/CFT risk, financial institutions may consider the following:

i. *Does the responsibility for oversight of AML/CFT identity and verification checks lie with management?*

ii. *Is senior management capable of meeting statutory obligations and ensuring that measures taken against ML/TF risks are sufficient and robust?*

iii. *Does management communicate AML/CFT issues with other business units?*

iv. *Is there regular reporting to senior management and by senior management to the Board on key AML/CFT issues?*

v. *Are there mechanisms in place for management to monitor and track AML/CFT issues to resolution?*

3.3. Client Risk

When completing question 1 of Section II of the ML/TF Risk Factor Assessment, in assessing the risk associated with clients, financial institutions may consider the following:

i. *What is the total number of clients as at the date of assessment?*

ii. *What are the target client markets and segments?*

iii. *What are the types of clients that the financial institution conducts business with e.g. institutional, retail, wealth management?*

iv. *The breakdown of different types of client by numbers.*

v. *What are the most common client structures of institutional clients?*

vi. *To what extent does the financial institution deal directly with individual clients?*

vii. *Number (%) of clients identified as high risk, including:-*

a. Clients with nationality or who are domiciled, clients incorporated or operating, in high risk jurisdictions.

b. Clients who are or beneficially own private members clubs.

c. *Clients who are politically exposed persons (PEPs).*

d. Clients who are correspondent banks.

e. Clients who are NPOs and identified as high risk.

f. *Clients that have had suspicions raised due to adverse media.*

g. *Number (%) of clients whereby suspicions have been raised with regard to their transactions and/ or fund transfers.*

h. *Corporate service providers (business entities and people that provide a range of services such as corporate advisory, office hosting, corporate secretarial services and statutory filings for their customer. e.g. lawyers, accountants, chartered secretaries and corporate secretarial agents).*

i. *Remittance service providers identified as high risk.*

j. *Any other client identified by the institution as high risk.*

3.4. Country Risk

When completing question 2 of Section II considerations for assessing country risk may include:

i. Evidence of adverse news or relevant public criticism of a country or jurisdiction, including FATF public documents on High Risk and Non-cooperative jurisdictions;

ii. Independent and public assessment of the country's or jurisdiction's overall AML/CFT regime, such as Mutual Evaluation reports and FSAP Reports for guidance on the country's or jurisdiction's AML/CFT measures;

iii. AML/CFT laws, regulations and standards of the country or jurisdiction consistent with those set by the FATF;

iv. Implementation of the standards (including quality and effectiveness of supervision) of AML/CFT, such as the level of control and/or regulation in the country or jurisdiction consistent with those set by FATF;

v. Whether the jurisdiction is a member of FATF;

vi. What is the nature of business/ background in country?

vii. List of different legal entities in country;

viii. Contextual factors of concern, such as political stability, maturity and sophistication of the regulatory and supervisory regime, level of corruption, financial inclusion, etc.;

ix. Which are the high risk countries that the financial institution exposed to through its clients, either through place of incorporation/ place of business for non-individual clients or their nationality/ place of domicile for individual clients?

x. Are there clients who reside in or with connections to high-risk jurisdictions;

xi. Does the financial institution and/or its branches/subsidiaries operate in in any high risk countries?

- Countries identified by the FATF/FSRB as jurisdictions with strategic AML/CFT deficiencies.
- Countries subject to sanctions, embargos or similar measures issued by international authorities.
- Countries that are believed to have strong links to terrorist activities.

- Countries identified by the OECD (Organisation for Economic Co-operation and Development) as a non-cooperative tax haven.
- Countries identified in the International Narcotics Control Strategy Report (INCSR) to be a "Jurisdiction of Primary Concern".

3.5. Products, Services and Delivery Channels

When completing question three of Section II, considerations for assessing the risk associated with products /services and delivery channels may include:

i. What are the different types of products and services offered?

ii. How do funds flow[62] into and out of the product/services and can payments be made by the client only or client and third party?

iii. What distribution channels are utilised? E.g. direct client relationships, indirect utilizing third party intermediaries or introducers;

iv. Can the product/service be established through non face-to-face channels?

v. Is reliance placed on CDD conducted by third parties? What arrangements are in place to ensure that the due diligence is conducted in accordance with the financial institution's policies and procedures?

vi. What payment processes are utilised? Are payments made to third parties?

vii. To what extent are the financial institution's product, services, transactions and delivery channels utilized by the potential higher risk customers identified in Section 3. above?

[62] Consider whether flows to and from product/service can be made via cash, cheques, domestic wires, international wires, ACH/RTGS, online banking; ATM

Part IV
Risk Based Customer Due Diligence

Part IV - Risk Based Customer Due Diligence

The guidance set out in this section has been adapted from the BCBS[63] and is intended to assist financial institutions in defining or refining their CDD approach. It may be utilized in respect of AML/CFT policies and procedures, especially in developing sound customer risk profiles. Financial institutions are reminded that an effective customer identification/verification programme should reflect the risks arising from the different types of customer, types of product/services and the varying levels of risk resulting from a customer's relationship with the financial institution.

Higher-risk customer relationships and transactions, such as those associated with PEPs or other higher-risk customers, will clearly require greater scrutiny than relationships and transactions associated with lower-risk customers. Therefore, these provisions should be read in conjunction with Sections 5 and 6 of Part II of this Guideline and the provisions related to assessing and understanding risks outlined in Part III of the Guideline.

The financial institution must identify the customer and all those who exercise control over the account / business arrangement. In this regard, a customer includes:

i. A person or entity that seeks to establish a relationship or has an existing relationship with the financial institution; or

ii. A person or entity on whose behalf a relationship is being established or an existing relationship is being maintained i.e. the beneficial owner. Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

1. IDENTIFICATION AND VERIFICATION OF INDIVIDUALS

For individuals, the information listed in Table 1, where applicable, should be obtained from the customer or from any other source for identification purposes.

Table 1 - Identification of Individuals who are Customers or Beneficial owners or Authorized Signatories

Minimum Information Requirements[64] (a)	**Potential additional information (on the basis of risk)**
Legal name (first and last name)	Any other names used (such as marital name, former legal name or alias);
Residential address[65]	Business address, post office box number, e-mail address and landline or mobile telephone numbers;
Nationality and an official personal identification number or other unique identifier[66]	Residency status
Date and place of birth	Name of employer, where applicable

[63] BCBS Guidelines – Sound Management of Risks related to Money Laundering and Financing of Terrorism 2016.

[64] All of this information may not be required in lower-risk situations, when simplified due diligence can be applied. The list also does not include other basic requirements, such as collecting signatures, which may be appropriate to support anti-fraud measures

[65] There are circumstances when this information is legitimately unavailable. This could prevent clients from accessing formal banking services. If clients are allowed to access to formal banking services, banks should apply mitigating measures as provided for by their internal risk policies, in line with regulatory requirements. Such measures could include utilising alternative information or conducting appropriate monitoring.

[66] See note 65 above.

Minimum Information Requirements[64] (a)	**Potential additional information (on the basis of risk)**
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected	Source and destination of funds passing through the account
Other information that may obtained, as applicable	
Occupation, public position held	
Income	
Financial products or services requested by the customer.	

1.1 Verification of identity of Individuals

The financial institution should verify the identity of the customer established through information collected in line with Table 1 above using reliable, independently sourced documents, data or information. The measures to verify the information produced should be proportionate to the risk posed by the customer relationship and should enable the financial institution to satisfy itself that it knows who the customer is.

1.2 Documentary Verification Procedures

Given the availability of counterfeit and fraudulently obtained documents, financial institutions should be aware that some identification documents are more vulnerable to fraud. In instances where there is uncertainty regarding the validity of the document(s) presented by the customer, the financial institution should conduct enhanced due diligence and verify the information provided by the customer by requesting additional documentary evidence of identity or by reviewing other sources of information.

Identification documents, either originals or certified copies, should be pre-signed and bear a discernable photograph of the applicant. Where prospective customers provide documents with which an institution is unfamiliar, either because of origin, format or language, the institution must take reasonable steps to verify that the document is indeed authentic, which may include contacting the relevant authorities or obtaining a notarized translation. In addition, where original documents are not available, the financial institution should only accept copies of documents that have been appropriately certified.

The following are some methods for verifying the identity of the customer. This list of examples is not exhaustive:

i. Confirming the physical identity of the customer or the beneficial owner from an unexpired official document (e.g. passport, identification card, residence permit, social security documents, driver's licence) that bears a photograph of the customer;

ii. Confirming the date and place of birth from an official document (e.g. birth certificate, passport, identity card, social security records);

iii. Confirming the validity of official documentation provided through certification by an authorized person (e.g. embassy official, public notary);

iv. Confirming the residential address (from a document no older than 6 months), utility bill excluding mobile phone bills, tax assessment, another financial institution's account statement, letter from a public authority;

v. Where a proposed account holder's address is temporary accommodation, for example an expatriate on a short term assignment, financial institutions should adopt

flexible procedures to obtain verification by other risk based means such as copy of contract of employment, or banker's or employer's written confirmation;

vi. Where the utility bill is not in the customer's name, the financial institution should request additional information to confirm the customer's address such as obtaining a letter from the landlord or a copy of the lease agreement and a recent receipt;

vii. In the case of students or other young people, the financial institution may consider verification using the home address of parent(s), or by making enquiries of the applicant's school or university;

viii. A recent mortgage statement from a recognized financial institution;

ix. Correspondence from a central or local government agency;

x. Confirming the permanent address by checking the Register of Electors;

xi. A documented record of a site-visit by an employee of the financial institution to the individual's residential address.

Financial institutions may also consider other verification procedures of an equivalent nature that will provide satisfactory evidence of a customer's identity and risk profile.

1.3 Non-documentary Verification Procedures

i. Contacting the customer by telephone or by letter to confirm the information supplied, after an account has been opened (e.g. a disconnected phone, returned mail etc. should warrant further investigation);

ii. Checking references provided by other financial institutions;

iii. Utilising an independent information verification process, such as by accessing public registers, private databases or other reliable independent sources (e.g. the Register of Electors or credit reference agencies);

iv. Given the increasing prevalence of social media data, financial institutions may consider taking such information into account as part of their CDD measures, but should have regard to the risks inherent in the reliability of this data.

1.4 Identification and Verification of Identity of Persons Appointed to Act on a Customer's Behalf

Financial institutions are reminded of the requirement to verify that any person purporting to act on behalf of the customer is authorized to do so in that capacity. Such authority to deal with assets on behalf of the financial institution's customer constitutes a business relationship and therefore, financial institutions must also identify and take reasonable measures to verify the identity of such persons.

This determination should be done prior to accepting instructions from that person. Appropriate documentary evidence of a customer's appointment of a natural person to act on its behalf includes legal authorization documents such as Powers of Attorney, a court issued judgement or equivalent document.

1.5 Acceptance of Certified Identification Documents

Financial institutions should exercise due caution when accepting certified copies of documents, especially where such documents originate from a country perceived to represent higher risk, or from unregulated entities in any jurisdiction. Where certified copies of documents are accepted, it is the institution's responsibility to satisfy itself that the certifier is authentic. The certifier[67] should sign the copy document (printing his name clearly underneath) and indicate his position or capacity on it together with a contact address, telephone and facsimile number and where applicable, a license/registration number.

In all cases, institutions should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document.

1.6 Further verification of information on the basis of risk

Particular attention needs to be focused on customers assessed as having higher-risk profiles. Additional sources of information and enhanced verification procedures may include:

i. Confirming an individual's residential address on the basis of official papers, a credit reference agency search, or through home visits;

ii. Prior bank reference (including banking group reference) and contact with the bank regarding the customer;

iii. Verification of income sources, funds and wealth identified through appropriate measures;

iv. Verification of employment and of public positions held; and

v. Personal reference (i.e. by an existing, credible customer of the same bank).

As part of its broader CDD measures, the financial institution should consider, on a risk-sensitive basis, whether the information regarding sources of wealth and funds or destination of funds should be corroborated.

2. IDENTIFICATION AND VERIFICATION OF LEGAL PERSONS AND ARRANGEMENTS AND BENEFICIAL OWNERSHIP

Financial institutions must identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure, with a view to establishing a customer risk profile.

2.1 Identification of Legal Persons

The term legal person[68] includes any entity (e.g. business or non-profit organization, distinct from its officers and shareholders) that is not a natural person or a legal arrangement. In considering the customer identification guidance for the different types of legal persons, particular attention should be

[67] Examples of suitable certifiers include a justice of the peace, notary public, police officer above the rank of sergeant and commissioners of affidavits.

[68] The FATF definition of 'legal person' refers to any entity other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This includes companies, bodies corporate and foundations, anstalt-type structures, partnerships or associations and other similar type entities.

given to the different levels and nature of risk associated with these entities. In the case of a partnership, each partner should be identified as well as the immediate family members with ownership control.

Companies sometimes form part of complex organizational structures which also involve legal arrangements such as trusts and foundations. Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. Financial institutions should take reasonable measures to look behind the corporate entity to identify those who have ultimate control over the business and the financial institution's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the financial institution. The financial institution should also ensure that any person purporting to act on behalf of the corporate entity is authorized to do so.

Table 2 – Identification of Legal persons

Minimum Information Requirements[69]	**Potential additional information (on the basis of risks)**
Name, legal form, status and proof of incorporation of the legal person;	
Permanent address of the principal place of the legal person's activities;	
Official identification number (financial institution registration number, tax identification number);	Legal entity identifier (LEI)[70] if available
Mailing and registered address of legal person;	Contact telephone and fax numbers.
Identity of natural persons who are authorized to operate the account. In the absence of an authorized person, the identity of the relevant person who is the senior managing official.	Identity of relevant persons holding senior management positions.
Nature and purpose of the activities of the legal entity and its legitimacy;	Financial situation of the entity;
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.	Sources of funds paid into the account and destination of funds passing through the account.
Identity of the beneficial owners[71]	
Powers that regulate and bind the legal person (such as the articles of incorporation for a corporation).	

There may be doubt as to the natural person(s) with controlling ownership interest or there is no natural person(s) exerting control through ownership interests. In such cases, the financial institution should identify those natural person(s) exercising control of the legal person or legal arrangement

[69] The list does not include other basic requirements such as collecting the signatures of the account holders.

[70] The LEI standard was developed by the International Organization for Standardization (ISO). It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. The publicly available LEI data pool can be regarded as a global directory, which greatly enhances transparency in the global marketplace. Subject to developments in the LEI project, this information may become required in the future. If unavailable, consider obtaining the company registration number.

[71] The term "beneficial owner" is used in this annex in a manner consistent with the definition and clarifications provided in the FATF standards. For reference, the FATF defines a "beneficial owner" as the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. If the financial institution is publicly listed on a recognized stock exchange and not subject to effective control by a small group of individuals, identification on shareholders is not required;

See Interpretative note to recommendation 10 of the FATF. See also FATF, *Transparency and beneficial ownership, October 2014, www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.*

through other means. Where no natural person is identified by the aforementioned, the financial institution should identify the relevant natural persons in senior managing positions or those exercising ultimate effective control over legal persons and arrangements, respectively. For legal persons, the information listed in Table 2 on the previous page should be collected for identification purposes.

2.2.2. Non-Documentary verification

i. Undertaking a financial institution search and/or other commercial enquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;

ii. Utilising an independent information verification process, such as credit agencies, KYC databases or other reliable independent sources (e.g. lawyers, accountants);

iii. Reviewing the financial institution's website and other public source information such as websites of regulators to determine if the entity is licensed or registered;

iv. Validating the LEI if available and associated data in the public access service and the companies registry ;

v. Obtaining bank references;

vi. Visiting the corporate entity, where practical;

vii. Contacting the corporate entity by telephone, mail or e-mail.

There may be other verification procedures of an equivalent nature that will provide satisfactory evidence of a customer's identity and risk profile.

2.2.3 Verification of identity of authorized signatories and of beneficial owners of Legal Persons

Financial institutions shall apply the requirements of Regulations 15 and 16 of the FOR *with appropriate and risk-based adaptation.* Financial institutions should verify that any person purporting to act on behalf of the legal person is so authorized and if so, verify the identity of that person. This verification should entail verification of the authorisation to act on behalf of the customer (a signed mandate, a court issued judgment or equivalent document).

Where there are several persons appointed to act on behalf of the customer (e.g. more than 10 authorized signatories), the financial institution should verify at a minimum those natural persons who will be dealing directly with the financial institution.

Documents that may assist with verification of authorized signatories and beneficial persons are:

i. Copies of Powers of Attorney, or any other authority, affecting the operation of the account given by the directors in relation to the financial institution duly supported by a copy of the respective Board Resolution;

ii. In the case of a formal partnership arrangement, there should be a mandate from the partnership authorizing the opening of an account.

Financial institutions should undertake reasonable measures to verify the identity of the beneficial owners in accordance with the FATF definition referenced in Table 3-Note (b), as well as verify

partners/controllers and authorized signatories in accordance with the due diligence procedures for individuals.

On the basis of risk, financial institutions may place reliance on information provided by the Corporate Secretary of the legal person on behalf of persons such as directors or where the company is a publicly listed company, publicly available information such as annual reports or information contained on their website may be used for non-documentary verification.

2.2.4 Further verification of information on the basis of risk

As part of its broader customer due diligence measures, the financial institution should consider, on a risk-sensitive basis, whether the information regarding financial situation and source of funds and/or destination of funds should be corroborated. For example, an institution may also review annual reports or request the financial statements of parent or affiliate companies, or seek evidence that the entity is not in the process of being dissolved or wound-up. It should request this information, particularly for non-resident companies, where the corporate customer has no known track record or it relies on established affiliates for funding.

2.3 Identification of Legal Arrangements

The term 'legal arrangement' used in this guidance is consistent with the definition provided by the FATF Standards i.e. express trusts or other similar legal arrangements such as *fiducie, treuhand* and *fideisomiso.* Financial institutions must inform the Central Bank when applicable laws and regulations in the domicile where the legal arrangement is established, prohibit the implementation of this guideline. The approval of the Central Bank to open an account for such customers is not required, but the Central Bank expects that the financial institution will conduct EDD before commencing the business relationship. For legal arrangements, the information in Table 3 should be obtained:

Table 3 - Legal Arrangements - Identification Information

Minimum Information Requirements[72]	**Potential additional information (on the basis of risk)**
Name of the legal arrangement and proof of existence;	Contact telephone and fax numbers if relevant;
Address and country of establishment;	
Nature, purpose and objects of the legal arrangement (e.g. is it discretionary, testamentary etc);	Legal entity identifier (LEI), if applicable[73]
The names of the settlor and the name of the person providing the funds if not the ultimate settler, the trustee(s), the protector/controller(s) (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement (including through a chain of control/ownership[74]	The names of the relevant persons having a senior management position in the legal arrangement, if relevant, addresses of trustees, beneficiaries.
Description of the nature and purpose/activities of the legal arrangement (e.g. in a formal constitution, trust deed);	Source of funds
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.	Origin and destination of funds passing through the account.

[72] The list does not include other basic requirements such as collecting the signatures of the account holders.

[73] Subject to developments in the LEI project, this information may be required in the future. If unavailable, consider obtaining the company registration number.

[74] Including the name of the individual who has the power (whether exercisable alone, jointly with another person or with the consent of another person) to: dispose of, advance, lend, invest, pay or apply trust property; vary the trust; add or remove a person as a beneficiary or to or from a class of beneficiaries; appoint or remove trustees; and direct, withhold consent to or veto the exercise of a power such as is mentioned in subparagraph (i), (ii), (iii) or (iv). In the case of a nominee relationship, the name of the beneficial owner(s).

2.4 Verification of Identity of Legal Arrangements

The financial institution should verify the identity of the customer established through information collected according to Table 5, using reliable, independently sourced documents, data or information. This includes at a minimum:

i. A copy of documentation confirming the nature and legal existence of the account holder (e.g. a certified copy of the deed of trust, register of charities); Where the settlor is deceased written confirmation should be obtained for the source of funds in the form, for example, of Grant of Probate, and/or copy of the will creating the trust;

ii. Where a corporate trustee acts jointly with a co-trustee, the identity of any non-regulated co-trustees should be verified.

Examples of other procedures of verification are given below. This list of examples is not exhaustive. There may be other procedures of an equivalent nature which may be produced, applied or accessed as satisfactory evidence of a customer's identity and risk profile, including:

i. Obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;

ii. Obtaining bank references;

iii. Accessing or searching public and private databases or other reliable independent sources.

2.4.1 Verification of Identity of authorized signatories and beneficial owners of the legal arrangement

Financial institutions should undertake reasonable measures to verify the identity of the beneficial owners of the legal arrangement. Financial institutions should verify that any person purporting to act on behalf of the legal arrangement is so authorized and if so, verify not only the identity of that person but also the person's authorisation to act on behalf of the legal arrangement (by means of a signed mandate, a court issued judgment or another equivalent document).

Depending on the type or nature of the legal arrangement, it may be impractical to verify all persons at the onset of the relationship e.g. in the case of unborn beneficiaries. In such cases, discretion should be exercised. In all circumstances however, there should be verification of beneficiaries before the first distribution of assets. Further, verification of protectors/ controllers should be undertaken the earlier of the first instance of exercise of power conferred by the trust instrument or the issue of instruction to an advisor to provide advice.

Verification should be made to ensure that any bank account on which the trustees have drawn funds is in their names, and the identities of any additional authorized signatories to the bank account should also be verified.

2.4.2 Further verification of information on the basis of risks

As part of its broader customer due diligence measures, ongoing due diligence should be applied in the context of changes in any of the parties to the trust, revision of the trust, addition of funds, investment of trust funds or distribution of trust assets/provision of benefits out of trust assets, including whether information regarding source of funds and/or destination of funds should be

corroborated. Where a trustee whose identity has been verified is replaced, the identity of the new trustee should be verified before the new trustee is allowed to exercise control over funds.

Any application to open an account, or undertake a transaction, on behalf of another without the applicant identifying a trust or nominee capacity should be regarded as suspicious and requires further enquiries.

Institutions should be particularly vigilant where there is no readily apparent connection or relationship of the settlor to the beneficiaries of a trust. Since the economic nature of a trust is a mechanism for the settlor to benefit a beneficiary, typically, not in return for any consideration (payment, transfer of assets or provision of services), institutions should endeavor so far as possible to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom he seemingly has no connection. This can be a matter of great sensitivity (for example where the beneficiary turns out to be a child of the settlor born out of wedlock) and institutions are encouraged to take this into account while pursuing necessary or appropriate inquiries.

There are a number of commercial structures in which a trust may feature as the legal owner, such as in debt repackaging arrangements. In such cases where the traditional relationship between the settlor and beneficiary is absent, institutions should demonstrate that they understand the commercial rationale for the arrangement and have verified the identity of the various counterparties.

3. THIRD PARTY RELIANCE

There may be circumstances in which obtaining and verifying customer information may be duplication and commercially onerous, for example, when an insurance broker refers business to an insurance company. Financial institutions may rely on third party financial institutions[75] for the performance of elements of customer due diligence. In such instances however, the ultimate responsibility and accountability remain with the financial institution that is placing reliance on the third party.

It is important to note that third party reliance is different from introduced business or an outsourcing arrangement. In a third party reliance scenario, the third party will typically have an existing relationship with the customer that is independent of the relationship to be formed by the customer with the relying financial institution. With respect to insurance agents and agents of a remittance company, the agent is viewed as an extension of the financial institution and consequently, the conduct of CDD by agents is treated as if conducted by the principal financial institution itself. The agents therefore adhere to the CDD requirements of the insurance company. In instances where the third party is a broker, the broker conducts CDD according to its own AML/CFT policies, procedures and controls.

In contrast, the outsourced service provider conducts certain activities (e.g. performs centralised transaction monitoring functions) on behalf of the financial institution, and is subject to the institution's control measures to effectively implement its AML/CFT procedures. In this regard, financial institutions that engage third parties, including payment service providers (PSP) to accept funds on their behalf, must ensure that the PSP has an appropriate AML/CFT risk management

[75] Regulation 11(1B) of the FOR

programme. Section 4.4 provides detailed information regarding the due diligence expectations for introduced business.

The basis for deciding to place reliance on a third party for CDD must be documented and approved by senior management.The third party being relied on should not itself present higher ML/TF risk such as being located in a jurisdiction that has been identified as having strategic AML/CFT deficiencies.

The relationship between financial institutions and the third parties relied upon to conduct CDD on their behalf should be governed by an arrangement such as the binding agreements between an insurance company and brokers or the agency arrangements between a remittance company and its agents, which clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, financial institutions must be satisfied that the third party:

i. has an adequate CDD process and that information collected clearly establishes the identity of the customer or beneficial owner and has been verified;

ii. has measures in place for record keeping requirements in accordance with the requirements in AML/CFT legislation and regulations;

iii. can provide the CDD information and provide copies of the relevant documentation immediately upon request; and

iv. is properly regulated and supervised.

Due consideration should be given to adverse public information about the third party, such as its subjection to an enforcement action for AML/CFT deficiencies or violations.

The decision to place reliance on a third party is not static and should be assessed regularly to ensure that it continues to conduct CDD in a manner as comprehensive as itself. For that purpose, the financial institution should randomly request details of changes in the CDD procedures of the third party and copies of CDD information and documents from a sample of customers to assess due diligence conducted, including screening against local databases to ensure compliance with local regulatory requirements. Financial institutions should consider refusing business from or terminating reliance on entities that do not apply adequate CDD on their customers or otherwise fail to meet requirements and expectations.

Prior to placing reliance on third parties in other jurisdictions, financial institutions must be satisfied that there are no laws in the jurisdiction in which the third party operates that would prohibit the fulfillment of the CDD obligations (e.g. bank secrecy laws).

4. CUSTOMER DUE DILIGENCE – SPECIFIC TYPES OF CUSTOMERS & ACTIVITIES

4.1 Politically Exposed Persons

Regulation 20 of the FOR defines a PEP as a person who holds or has held one of the following offices or positions domestically in Trinidad and Tobago or *its equivalent in a foreign country*. The definition of a PEP is not intended to cover middle ranking or more junior individuals.

i. heads of state and heads of government;

ii. persons elected to office in national or local or the Tobago House of Assembly elections;

iii. persons appointed to serve:

- as a Senator in the Trinidad and Tobago Parliament or
- on the Tobago House of Assembly; or
- as an Alderman in a Municipality or Regional Corporation.

iv. A Permanent Secretary or any other person appointed as an Accounting Officer under the Exchequer and Audit Act or individuals holding equivalent positions in a foreign jurisdiction;

v. Senior judicial or military officials;

vi. The chairman, deputy chairman, president or vice-president of the Board of Directors of a state-owned corporation; the managing director, general manager, comptroller, secretary or treasurer of a state owned corporation; or any duly appointed person holding the equivalent position in a state owned corporation;

vii. The chairman, deputy chairman, secretary and treasurer of a political party or individuals holding equivalent positions in a foreign country;

viii. Persons who are or have been entrusted with a prominent position by an international organization[76] such as directors and members of the board or equivalent functions.

Immediate family members such as parents, siblings, spouses, and children and close associates of the PEP may also benefit from or be used to facilitate abuse of public funds by the PEP and are also considered to be PEPs.

Some examples of a close associate may include a person who is:

i. business partner with, or who beneficially owns or controls a business with a PEP;

ii. publicly known or actually known to be in a romantic relationship with a PEP;

iii. involved in financial transactions with a PEP;

iv. a prominent member of the same political party as a PEP; or

v. closely carrying out charitable works with a PEP.

These are examples to assist financial institutions in identifying close associates. It is not contemplated that every person associated with a PEP will be considered a close associate. Financial institutions may consider factors such as the level of influence the PEP has on such a person or the extent of the close associate's exposure to and influence on the PEP. The institution may rely on information available from public sources to identify an individual who is widely and publicly known to maintain a close relationship with PEP, either socially or professionally.

[76] An international organization is an organization set up by the governments of more than one country by means of a formally signed agreement between the governments and have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident organizations of any of the countries in which they are located. See also the Glossary of the FATF Standards and Appendix II of this Guideline.

Financial institutions must take reasonable measures to determine whether a person is a PEP. Reasonable measures include, but are not limited to, one or more of the following actions:

i. Asking the customer at inception of the relationship. The customer's occupation or employment obtained at the time of account opening or during the ongoing due diligence process is a key factor in PEP determination or self-disclosure of PEP status by the customer;

ii. Conducting an open source search. Use the internet and media as sources of information for the determination, monitoring, verification of information in relation to PEPs, noting that information retrieved may not in all cases be comprehensive or reliable;

iii. Consulting a source of commercially available information. Financial institutions must consider the imitations of such databases noting that use of these databases should never replace risk based CDD processes.

A combination of measures may be used to make the PEP determination. It is expected that the financial institution will have proactive measures in place to make the determination. For example, account opening procedures may include a specific question on PEP status and/or capture occupation to identify holders of public office. It is important that financial institutions periodically monitor their existing client base against changes in the PEP universe and not just at the time of client on-boarding. Outside of periodic screening, the financial institution may also rely on media monitoring to identify PEPs. For example, newspaper announcements regarding changes to board members of state owned corporations. Additional sources of information include the Parliament website and the Tobago House of Assembly website; the FIU website for the list of Accounting Officers appointed under the Exchequer and Audit Act; the Ministry of Finance website (for information on Boards of state-owned entities); the website of the Judiciary of the Republic of Trinidad and Tobago; the website of the Ministry of Rural Development & Local Government; and 'ttconnect' for diplomatic representatives and honorary consuls in Trinidad and Tobago. Appendix II provides an additional list of websites that may be used to support PEP identification for heads of an international organization.

In line with Part III of this Guideline, the assessment of the relationship may take into account, among other factors i) customer risk factors, ii) country risk factors, and iii) product, service, transaction or delivery channel risks. Additional factors to be taken into account should include the nature of the prominent public function that the PEP has, such as level of seniority, access to or control over public funds and the level of authority over policy, operations or the use or allocation of government-owned resources or the ability to direct the award of government contracts; the nature of title (honorary or salaried political function) and whether the PEP has links to an industry that is particularly prone to corruption. Sections 4.1.3and 4.1.4 provide a list of potential higher and lower risk indicators relative to PEPs.

Due diligence measures may include:

i. Understanding and documenting the length of time, the title or position and country in which the PEP holds, or held, political exposure;

ii. If the individual customer is a close family member or close associate, the relationship of the person to the PEP must be documented;

iii. Understanding and documenting the nature and intended purpose of the relationship/account, the source of the initial funds (where appropriate) and the anticipated levels of account activity;

iv. Understanding and documenting the customer's source of funds and source of wealth (e.g. salary and compensation from official duties and wealth derived from other sources). Where the risks are high or there are doubts as to the veracity of the information provided by the customer, financial institutions should validate this information using independent and reliable sources;

v. Conduct Negative News/Adverse Media screening on the customer and evaluate any positive hits.

4.1.1 Enhanced Due Diligence Measures for PEPs

Part II of this Guideline provides examples of enhanced measures that may be applied to a high risk PEP relationship.

4.1.2 Simplified Due Diligence Measures

In addition to the steps provided in Section 6.3 of Part II of this Guideline, the following are examples of measures that may be appropriate for PEPs assessed to be lower risk:

i. Take less intrusive and less exhaustive steps to establish the source of wealth and source of funds; for example, only use information already available to the institution (such as transaction records or publicly available information) and do not make further inquiries of the individual unless anomalies arise;

ii. Oversight and approval of the relationship takes place at a less senior level of management;

iii. Re-assess the risk associated with the relationship after a reasonable period of time has passed since the PEP demitted public office and consider appropriate due diligence measures. Changes to risk profiles must be comprehensively documented and appropriately approved; and

iv. Apply less frequent formal review and monitoring of the relationship.

4.1.3 Higher Risk Indicators for PEPs

This is not an exhaustive list; other factors may suggest higher risk as new corruption typologies develop:

1) <u>Geographical</u>

A PEP may pose a greater risk if she/he is from, or closely connected to, a country with some of the following characteristics:

- associated with high levels of corruption
- political instability
- weak state institutions
- weak anti-money laundering defences

- armed conflict
- non-democratic forms of government
- widespread organised criminality
- a political economy dominated by oligopolistic actors with close links to the state
- lacking a free press and where legal or other measures constrain journalistic investigation
- a criminal justice system vulnerable to political interference
- lacking expertise and skills related to book-keeping, accountancy and audit, particularly in the public sector
- law and culture antagonistic to the interests of whistle-blowers
- weaknesses in the transparency of registries of ownership for companies, land and equities

2) Personal and Professional

A politically exposed person may pose a higher risk if she/he has any of the following characteristics:

- personal wealth or lifestyle inconsistent with known legitimate sources of income or wealth
- subject to credible allegations of financial misconduct (e.g. facilitated, made, or accepted bribes)
- there is evidence they have sought to disguise the nature of their financial circumstances
- is responsible for, or able to influence, large public procurement exercises, particularly where procurement is not subject to competitive tender, or otherwise lacks transparency
- is responsible for, or able to influence, allocation of scarce government licenses such as a mineral extraction concessions or permission for significant construction projects.

4.1.4 Lower Risk Indicators for PEPs

1) Geographical

A PEP may pose a lower risk if he/she solely operates in a country that has the following characteristics:

- associated with low levels of corruption
- political stability and free and fair elections
- strong state institutions

- credible anti-money laundering defences
- a free press with a track record for probing official misconduct
- an independent judiciary and a criminal justice system free from political interference
- a track record for investigating political corruption and taking action against wrongdoers
- strong traditions of audit within the public sector
- legal protections for whistle-blowers
- well-developed registries for ownership of land, companies and equities

2) Personal and Professional

A PEP may pose a lower risk if he/she has the some of the following characteristics:

- is subject to rigorous disclosure requirements (such as registers of interests, independent oversight of expenses)
- does not have executive decision-making responsibilities (such as a government MP with no ministerial brief or an opposition MP)
- has ceased to be a PEP for an extended period of time and the financial institution is comfortable that he no longer wields political influence.

4.1.5 High risk indicators in respect of a PEP's family or known close associate

The family and close associates of a politically exposed person may pose a higher risk if they have any of the following characteristics:

- Wealth derived from the granting of government licences (such as mineral extraction concessions, licence to act as a monopoly provider of services, or permission for significant construction projects).
- Wealth derived from preferential access to the privatisation of former state assets
- Wealth derived from commerce in industry sectors associated with high-barriers to entry or a lack of competition, particularly where these barriers stem from law, regulation or other government policy
- Wealth or lifestyle inconsistent with known legitimate sources of income or wealth
- Subject to credible allegations of financial misconduct (e.g. facilitated, made, or accepted bribes)
- Appointment to a public office that appears inconsistent with personal merit

4.2 Foundations

A foundation (also a charitable foundation) is a legal characterization of a non-profit organization (NPO) that will typically either donate funds and support to other organizations, or provide the source of funding for its own charitable purposes. A private foundation is a legal entity set up by an individual, a family or group of individuals for a purpose such as philanthropy. Unlike a charitable foundation, a private foundation does not generally solicit funds from the public. In the case of foundations, financial institutions should obtain information on:

i. The foundation's charter;

ii. The certificate of registration or document of equivalent standing in a foreign jurisdiction should be obtained in order to confirm the existence and legal standing of the foundation;

iii. The source of funds. In cases where a person other than the founder provides funds for the foundation, institutions should verify the identity of that third party providing the funds for the foundation and/or for whom a founder may be acting;

iv. The identification evidence for the founder(s) and for officers and council members of a foundation as may be signatories for the account(s) of the foundation; and

v. The identification evidence should also be obtained for all vested beneficiaries of the foundation.

4.3 Executorships

Where a business relationship is entered into for the purpose of winding up the estate of a deceased person, the identity of the executor(s)/ administrator(s) of the estate should be verified. However, the identity of the executor or administrator need not normally be verified when payment from an established bank account in the deceased's name is being made to the executor or administrator in accordance with the Grant of Probate or Letters of Administration solely for the purpose of winding up the estate. Payments to the underlying beneficiaries on the instructions of the executor or administrator may be made without verification of their identity.

4.4 Introduced Business

A financial institution may rely on other regulated third parties to introduce new business in whole or in part, for example, insurance agents. Nevertheless, the ultimate responsibility remains with the financial institution for customer identification and verification that the documentary evidence of the introducer that is being relied upon, is satisfactory for these purposes.

Financial institutions should therefore:

i. Document in a written agreement, such as the binding agreements between the insurance company and agents, the respective responsibilities of the two parties;

ii. Where the introducer is a financial entity, satisfy itself that the regulated entity or introducer has in place KYC/ CDD practices at least equivalent to those required by Trinidad and Tobago law and the financial institution;

iii. Obtain copies of the due diligence documentation provided to the introducer within a reasonable time frame subsequent to the commencement of the business relationship; and

iv. Consider terminating the relationship with an introducer who is not within the financial institution's group, where there are persistent deviations from the written agreement and where an introducer fails to provide the requisite customer identification and verification documents.

A foreign financial institution may act as an introducer if:

i. It is an entity regulated by a regulatory or supervisory body equivalent to the Central Bank or the TTSEC;

ii. It is based in a country subject to equivalent or higher AML/ CFT standards of regulation; and

iii. There are no obstacles which would prevent the financial institution from obtaining the original documentation.

Reliance on an eligible introducer should be approved by senior management and the decision as to whether normal due diligence procedures are followed should be part of the financial institution's risk-based assessment.

Notwithstanding any reliance on an eligible introducer's CDD procedures, financial institutions should ensure that they receive all the relevant information pertaining to a customer's identity within a reasonable timeframe. Financial institutions should have clear and legible copies of all documentation in their possession within thirty days of receipt of the written confirmation of the eligible introducer that they have verified customer identity in accordance with their national laws. The eligible introducer must certify that any photocopies forwarded are identical with the corresponding originals. This certification should be provided by a senior member of the introducer's management team. If documents are not obtained within 30 days of receipt of the introducer's written confirmation, the account should be suspended and if after a further reasonable period, the financial institution still does not receive the documents, the business relationship should be terminated.

4.4.1 Introduced Business by Companies within a Financial Institution's Group

When a prospective customer is introduced from within a financial institution's group, it is not necessary to re-verify the identification documents unless doubts subsequently arise about the veracity of the information. This is provided that the identity of the customer has been verified by the introducing regulated parent financial institution, branch, subsidiary or associate in line with the standards set out in this Guideline.

Financial institutions should obtain written confirmation from the group member confirming completion of verification and retain copies of the identification records in accordance with the requirements in the FOR.

Where a financial institution or its subsidiary initiates transactions without establishing face-to-face contact and obtaining all of the relevant documentation, it should make all efforts to obtain such information as soon as possible. In accepting such transactions, institutions should:

i. Set limits on the number and aggregate value of transactions that can be carried out;

ii. Indicate to customers that failure to provide the information within a set timeframe, may trigger the termination of the transaction; and

iii. Consider submitting a suspicious activity report (SAR).

4.4.2 Introduced Business by Professional Service Providers

Professional service providers act as intermediaries between clients and the financial institution and such persons include lawyers, accountants and other third parties that act as financial liaisons for their clients.

When establishing and maintaining relationships with professional service providers, a financial institution should:

i. Adequately assess the account risk and monitor the relationship for suspicious or unusual activity;

ii. Determine whether the person is duly registered under relevant legislation e.g. insurance agents and brokers under the IA, brokers and dealers under the Securities Act Chapter 83:02 etc.;

iii. Understand the intended use of the account, including the anticipated transaction volume, products and services used, and geographic locations involved in the relationship; and

iv. Obtain the identity of the beneficial owners of the client funds where it is not satisfied that the intermediary has in place due diligence procedures equivalent to the standard of this Guideline.

4.5 Private Banking

Institutions that offer private banking services for high net worth individuals must ensure that EDD policies and procedures are developed and clearly documented in the overall KYC policy to govern this area of operations. Similar to PEPs, senior management with ultimate responsibility for private banking operations should ensure that the personal circumstances, income sources and wealth of private banking clients are known and verified as far as possible, and should also be alert to sources of legitimate third party information. The approval of private banking relationships must be obtained from at least one senior level officer, other than the private banking officer/relationship manager.

4.6 Employee Benefit Programmes

Where an occupational pension programme, employee benefit trust, savings plan or share option plan is an applicant for an account, the trustee and any other person who has control over the relationship (e.g. administrator, sponsor or account signatories) can be considered as beneficial owners and the financial institution should take steps to identify them and verify their identities.

4.7 Mutual Funds, Friendly Societies, Cooperatives and Provident Societies

Where these entities are applicants for accounts, those persons exercising control or significant influence over the organisation's assets should be considered the beneficial owners and therefore identified and verified. This should include board members as well as executives and account signatories.

4.8 Professional Intermediaries

When a professional intermediary opens a customer account on behalf of a single customer that customer must be identified. Professional intermediaries will often open "pooled" accounts on behalf of a number of clients. Where funds held by the intermediary are not co-mingled but "sub-accounts" are established which can be attributed to each beneficial owner, all beneficial owners of the account held by the intermediary should be identified. Where the funds are co-mingled, the financial institution should look through to the beneficial owners. In these instances and on the basis of risk, the financial institution may consider whether the professional intermediary is supervised as a listed business by the FIU or where the intermediary is subject to due diligence standards in respect of its customer base that are equivalent to those applying to the financial institution itself, such as may be the case for broker-dealers).

Where an account is opened for an open or closed-end investment financial institution, unit trust or limited partnership that is subject to[77] customer due diligence requirements which are equivalent to those applying to the financial institution itself, the investment vehicle may be considered the customer and steps taken to identify and verify:

i. The fund itself;
ii. Its directors or any controlling board where it is a financial institution;
iii. Its trustee where it is a unit trust;
iv. its managing (general) partner where it is a limited partnership;
v. Account signatories; and
vi. Any other person who has control over the relationship e.g. fund administrator or manager.

4.9 Correspondent Banking

Correspondent banking is the provision of banking services by one bank in Trinidad and Tobago ("the correspondent bank") to another bank ("the respondent bank") in a foreign country. Correspondent banking relationships are established between banks to facilitate, among other things, transactions between banks made on their own behalf; transactions on behalf of their clients; and making services available directly to clients of other banks. The correspondent does not normally have a business relationship with the respondent's customers and will not normally know their identity or the nature or purpose of the underlying transaction, unless this is included in the payment instruction.

Examples of these services include inter-bank deposit activities, international electronic funds transfers, cash management, cheque clearing and payment services, collections, payment for foreign exchange services, processing client payments (in either domestic or foreign currency) and payable-through accounts.

Financial institutions must apply appropriate levels of due diligence to such accounts by gathering sufficient information from and performing enhanced due diligence processes on correspondent banks prior to setting up correspondent accounts.

[77] Consideration may also be given to whether the institution is supervised by another SA such as the SEC.

Regulations 21 and 22 of the FOR outline specific requirements for correspondent banks prior to their establishing relationships with a respondent bank. There is no expectation that correspondents apply CDD measures to the respondent's individual customers. The due diligence process prior to the establishment of a correspondent banking relationship should involve:

i. Obtaining authenticated/ certified copies of Certificates of Incorporation and Articles of Association (and any other financial institution documents to show registration of the institution within its identified jurisdiction of residence) ;

ii. Obtaining authenticated/certified copies of banking licences or similar authorization documents, as well as any additional licences needed to deal in foreign exchange;

iii. Determining the supervisory authority which has oversight responsibility for the respondent bank;

iv. Determining the ownership of the financial institution;

v. Obtaining details of respondent bank's board and management composition;

vi. Determining the location and major activities of the financial institution;

vii. Reviewing FATF notices or (or FATF style regional body's) mutual evaluation report or other assessment of the home country's measures to implement the FATF Recommendations;

viii. Establishing and periodically update an AML country risk rating system and assign a rating to each country in which a correspondent banking relationship has been established, for the purpose of implementing an appropriate level of monitoring;

ix. Ensuring that the documentation of the agreement includes an obligation to provide relevant customer identification information when requested to do so;

x. Obtaining details regarding the group structure within which the respondent bank may fall, as well as any subsidiaries it may have;

xi. Obtaining proof of its years of operation, along with access to its audited financial statements (5 years if possible);

xii. Information on its external auditors;

xiii. Ascertaining whether the bank has established and implemented sound customer due diligence, anti-money laundering and anti-terrorism financing policies and strategies and appointed a CO (at senior management level), inclusive of obtaining a copy of its AML/CFT policy and guidelines;

xiv. Ascertaining whether the correspondent bank has in the previous 7 years (from the date of the commencement of the business relationship or negotiations therefore), been the subject of or is currently subject to any regulatory action or any AML/CFT prosecutions or investigations;

xv. Establishing the purpose of the correspondent account;

xvi. Documenting the respective responsibilities of each institution in the operation of the correspondent account; and

xvii. Identifying any third parties that may use the correspondent banking services.

A financial institution is prohibited from entering or continuing a correspondent banking relationship with a shell bank. A shell bank is a bank that has no physical presence in the county in which it is incorporated and licensed and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Consequently, financial institutions will need to satisfy themselves that the foreign respondent banks do not permit their accounts to be used by shell banks. This may include asking the respondent for confirmation that they do not deal with shell banks, having sight of relevant passages in the respondents' policies and procedures or considering publicly available information, such as legal provisions that prohibit the servicing of shell banks. Financial institutions may also consider whether:

i. The respondent bank permits "payable through accounts". This would be one likely way in which shell banks could take advantage of respondent banks;

ii. The respondent bank's inability or reluctance to provide ultimate beneficiary/customer information in relation to pooled arrangements or collective investment schemes or aggregate accounts whereby only the KYC on the agent of the beneficiaries of the pooled arrangement, collective investment scheme or aggregate account will be or can be provided by the respondent bank; and

iii. The country in which the foreign respondent bank resides; whether there are secrecy laws that prohibit the release of any KYC information or which laws present an obstacle to the KYC due diligence process.

4.10 Payable-Through Accounts

Payable-through accounts refer to correspondent accounts that are used directly by third parties to transact business on their own behalf. In this regard, banks must be guided by requirements under Regulation 21(3) (c) of the FOR and the criteria established in this Guideline for introduced business.

Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf. FATF also requires financial institutions that use payable through accounts to apply enhanced due diligence measures in addition to normal measures.

4.11 Wire/funds transfers

A wire or funds transfer refers to any transaction carried out on behalf of an originator[78] through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at another financial institution. The originator and beneficiary may be the same person. Beneficiary refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.

Financial institutions that provide money remittance services must comply with all the relevant requirements as outlined in the preceding paragraphs. Money remitters should also refer to Section C of Part V of this Guideline for sector specific guidance.

Financial institutions must ensure that the relevant originator and beneficiary information accompany and remain with the wire transfer throughout the payment chain as set out in Regulations 33 and 34 of

[78] The originator is the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

the FOR. For occasional cross-border wire transfers below TTD 6,000 the name of the originator and of the beneficiary will be requested, as well as an account number for each or a unique transaction reference number; however such information will not have to be verified unless there are suspicious circumstances related to ML/TF, in which case information pertaining to customer should be verified.

The requirements are not applicable to the following types of payments:

a) Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, the necessary information should be included in the message; and
b) Financial institution-to-financial institution transfers where both the originator and the beneficiary are financial institutions acting on their own behalf.

When serving as intermediary or beneficiary financial institutions, financial institutions should have risk-based policies and procedures which include: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

PART V
SECTOR SPECIFIC GUIDANCE

Part V - Sector Specific Guidance

The following sections must be read in conjunction with Parts II and IV of this Guideline. Please note that the risk factors described in each section are not exhaustive. Financial institutions should take a holistic view of the risk associated with the situation, and note that isolated risk factors do not necessarily move a business relationship or occasional transaction into a higher or lower risk category.

In addition to the guidance provided in Parts II and IV of this Guideline, additional examples of CDD measures that financial institutions may apply on a risk-sensitive basis are provided. . These examples are not exhaustive and financial institutions should decide on the most appropriate CDD measures to apply taking into consideration the level and type of ML/TF risk they have identified.

A. Sector Specific Guidance for Licensees under the Financial Institutions Act, 2008

Due to the nature of the products and services offered, the relative ease of access and the often large volume of transactions and business relationships, banks are vulnerable to ML and TF. At the same time, the volume of business relationships and transactions associated with retail banking can make identifying money laundering and terrorist financing risk associated with individual relationships and spotting suspicious transactions more challenging.

Licensees should consider the following risk factors and measures in developing its risk based Compliance Programme in accordance with Parts II and III of this Guideline.

1. Product, service and transaction risk factors

The following factors may indicate higher risk:

i. The product's features might favour anonymity;

ii. The product allows payments from unidentified or un-associated third parties where such payments would not be expected, for example for mortgages or loans;

iii. The product places no restrictions on turnover, cross-border transactions or similar product features;

iv. New products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products in particular where these are not yet well understood;

v. A high volume or large value of transactions.

Lower risk is associated with products with limited functionality, for example:

i. A fixed term savings product with low savings thresholds;

ii. A product where the benefits cannot be realised for the benefit of third persons or are only realisable in the long term;

iii. A low value loan facility where the legal and beneficial title to the asset is not transferred to the customer until the contractual relationship is terminated;

iv. A financial inclusion product that can only be held by certain categories of customers, *e.g.* pensioners or benefit recipients, parents on behalf of their children, minors until they reach the age of majority, etc.;

v. There is no pre-payment facility.

2. Customer risk factors

The following factors may indicate higher risk:

i. The nature of the customer, for example:

- The customer is a cash-intensive undertaking;
- The customer is an undertaking associated with higher levels of ML/TF risk, for example money remittance and gambling businesses;
- The customer is an undertaking associated with a higher corruption risk, for example construction, extractive industries or arms trade;
- The customer is a non-profit organisation that supports jurisdictions associated with an increased terrorist financing risk, conflict zones etc;
- The customer is a new undertaking without adequate business profile or track record;
- The customer is a non-resident;
- The customer's beneficial owner cannot easily be identified, for example because the customer's ownership structure is unusual, unduly complex or opaque or because the customer issues bearer shares.

ii. The customer's behaviour, for example:

- The customer is reluctant to provide CDD information or appears deliberately to avoid face to face contact;
- The customer's behaviour or transaction volume is not in line with that expected from the category of customer to which he belongs, or is not expected based on the information the customer provided at account opening;
- The customer's behaviour is unusual, for example the customer unexpectedly and without reasonable explanation accelerates an agreed repayment schedule, either by means of lump sum repayments, or early termination; deposits or demands pay-out of high-value bank notes without apparent reason; increases activity after a period of dormancy, or makes transactions that appear to have no economic rationale.

The following factors may indicate lower risk:

i. The customer is a long-standing client whose previous transactions have not given rise to suspicion or concern, and the product or service sought is in line with the customer's risk profile;

ii. The customer is a public financial institution listed on a regulated market and is subject to disclosure requirements that ensure adequate transparency of beneficial ownership;

iii. The customer is a domestic public administration or enterprise or a public administration or enterprise from a jurisdiction with low levels of corruption;

iv. The customer is a credit or financial institution from a jurisdiction with an effective AML/CFT regime and is supervised for compliance with their AML/CFT obligations.

3. Country or Geographic Risk Factors

The following may indicate higher risk:

i. The customer has significant personal or business links to high risk countries, including those identified by the FATF, CFATF and other FSRBs as having strategic AML/CFT deficiencies and jurisdictions with higher levels of predicate offences such as those related to the narcotics trade, smuggling, corruption and counterfeiting.

The following may indicate lower risk:

i. Countries associated with the transaction have an AML/CFT regime comparable to that required under the FOR and are associated with low levels of predicate offences / healthy ML/TF conviction and confiscation records.

4. Distribution Channel Risk Factors

The following factors may indicate higher risk:

i. Non-face to face business relationships and services where no additional safeguards are in place;

ii. Reliance on a third party's CDD measures in situations where the bank does not have a long-standing relationship with the referring third party;

iii. New delivery channels that have not been tested yet.

A.1. Guidance for Banks When Providing Banking Services to Money Remitters

This guidance sets forth the minimum steps that banks should take when providing banking services to money remitters. Money remitters should be prepared to provide certain information and documentation as outlined in this guidance, when seeking to open or maintain account relationships with banks.

This guidance also seeks to assist banks in assessing and minimizing the risk of money laundering posed by individual money remittance customers. While banks are expected to manage risk associated with all accounts, banks will not be held responsible for their customers' compliance with AML/CFT legislative and regulatory requirements.

As noted in Part II of this Guideline, the Central Bank expects commercial banks to take a risk-based approach to assessing customer relationships on a case by case basis, rather than declining to provide banking services to entire categories of customers.

1. Risk Assessment

The risk inherent in the money remittance sector is not the nature of the sector itself, but the sector's vulnerability to abuse by criminals. Banks need to understand these potential risks and manage them effectively. Risk indicators to consider where assessing customer risk include:

i. Reluctance by the money remitter to provide CDD information on owners and principals of the business or regarding specific customers when requested by the bank;

ii. Acceptance of false identification and fictitious names from customers;

iii. Turnover of the business exceeding, to a large extent, the cash flows of other comparable businesses in the sector;

iv. Suspicious connections of the owner;

v. Suspicious transactions performed on the bank accounts of the business or its owner;

vi. Overly complicated agent/principal networks with inadequate oversight by principal.

In this regard, banks should determine whether its customer is a principal in its own right, or whether it is itself an agent of another money remitter. Money remitters that operate as principals or through a limited number of offices/agents, present a different risk profile from those that operate through a network of agents. It is important to understand the way the latter type of money remitter monitors and confirms compliance by its agents with its AML/CFT compliance programme.

1.1 Minimum Due Diligence Requirements

It is expected that banks that open and maintain accounts for money remitters will apply AML/CFT due diligence requirements as they do with all customers, on a risk sensitive basis. As a financial institution subject to AML/CFT requirements, a money remitter is subject to the full range of AML/CFT controls with which it has to comply vis-à-vis its customers, such as: CDD, wire transfer rules, record-keeping and ongoing monitoring mechanisms, etc.

It is therefore reasonable and appropriate for a bank to review the AML/CFT measures of the money remitter as part of the overall customer risk assessment before on-boarding the money remitter as a customer. Additionally, it is reasonable and appropriate that the money remitter should provide:

i. Evidence of registration with the FIU;

ii. Confirmation that it has conducted the relevant agent due diligence (where applicable);

iii. Confirmation that its AML/CFT program includes its agents and that compliance is monitored.

When assessing the risks associated with money remitters, important risk elements to consider include the scope of markets served (domestic or international), the purpose of the bank account and the anticipated account activity, the effectiveness of regulatory oversight in the countries of operation (where the principal is an internationally based remittance financial institution) and the effectiveness of the its risk management and compliance programs.

1.2 Maturity of the business and its owner's experience

It is relevant to consider whether or not the money remitter is a new or established operation, the level of experience the management and those running the business have in this type of activity, and whether or not providing money remittance services is the customer's primary or an ancillary business.

1.3 Anticipated account activity

Banks should ascertain the expected services that the money remitter will use, such as currency deposits or withdrawals, cheque deposits, or funds transfers. A money remitter may only operate out of one location and use only one branch of the bank, or may have several agents making deposits at multiple bank branches. Banks should also have a sense of expected transaction amounts.

1.4 Purpose of the account

As for all customers, understanding the purpose of the account is a critical element of the due diligence process. A money remitter might require the bank account to remit funds to its principal's settlement account. Accounts related to the remittance business should be separate from accounts used for the operational administration of the business itself.

Depending on the bank's risk assessment, information that might be relevant to obtain may include some or all of the following:

i. The expected source and destination of the funds to be used in the relationship;

ii. The origin of the initial and on-going source(s) of wealth and funds of the money remitter;

iii. Copies of recent and current financial statements;

iv. Understanding of the various relationships between signatories and with underlying beneficial owners.

In the light of the risk it perceives in the proposed customer, the bank may include consideration of matters such as:

i. The money remitter's public disciplinary record, to the extent that this is available;

ii. The nature of its customers, the product/service sought and the values and volumes involved;

iii. The anticipated level and nature of the activity that is to be undertaken through the relationship, on each account to be opened;

iv. The settlement arrangements with its US clearing banks.

1.5 Enhanced Due Diligence

Depending on the level and nature of risk identified, and the size and sophistication of the particular money remitter, banks may pursue other avenues as part of an appropriate due diligence process. When identified risks are higher, enhanced due diligence should be applied, which may include reviewing the AML/CFT (group-wide) programmes, the internal or external audit and other reports, review of the list of agents and their monitoring, the management and screening practices. A visit to the place of business, where appropriate, may prove helpful to check the existence and activities of the customer.

1.6 Ongoing monitoring

Based on the bank's risk assessment, monitoring should include periodic confirmation that initial projections of account activity have remained reasonably consistent over time. Risk-based monitoring generally does not include "real-time" monitoring of all transactions flowing through the account.

Examples of unusual activity across accounts, that may or may not be potentially suspicious generally involve significant and unexplained variations in transaction size, nature, or frequency through the account, such as:

i. Transferring funds to a different jurisdiction than expected based on the due diligence information collected. For example, if the customer indicated to the bank or in its business plan that it specializes in remittances to Latin America and the Caribbean and starts transmitting funds on a regular basis to conflict zones;

ii. A money remitter deposits currency significantly in excess of expected amounts, without any justifiable explanation, such as an expansion of business activity, new locations etc.

1.7 Risk Indicators

The following are examples that may be indicative of lower and higher risk to assist banks in their determination of the level of risk posed by a money remitter as a customer. This list is not intended to be prescriptive or exhaustive and a bank should not take any single indicator as definitive of the existence of lower or higher risk. Any conclusions regarding the risk profile should be based on a comprehensive consideration of all available information.

*1.7.1 Examples of potentially lower risk indicators***:**

The money remitter:

i. Primarily markets to customers that conduct routine transactions with moderate frequency in low amounts;

ii. Is an established business with a known operating history;

iii. Only remits funds to domestic entities; or primarily facilitates domestic bill payments.

1.7.2 Examples of potentially higher risk indicators:

The money remitter:

i. Allows customers to conduct higher-amount transactions with moderate to high frequency;

ii. Is a money transmitter that offers primarily, cross-border transactions, particularly to jurisdictions posing heightened risk for money laundering or the financing of terrorism or to countries identified as having weak anti-money laundering controls;

iii. Is a new business without an established operating history;

iv. Is a relatively small concern, with few employees but is a principal with a large agent network - this mitigates against effective supervision and control of agents;

v. Has agents who have agents of their own, or the principal is itself an agent of another business.

B. SECTOR SPECIFIC GUIDANCE FOR REGISTRANTS UNDER THE INSURANCE ACT CHAP 84:01

The following risk factors and measures must be read in conjunction with the main guidance set out in Part II and Part IV of this Guideline.

The National Risk Assessment concluded that certain classes of insurance, namely general, health and term life, present low ML/TF risk. Additionally, the FATF Standards in respect of the insurance sector apply to the underwriting and placement of life insurance and other investment related insurance. In accordance with a risk based approach, the application of simplified due diligence in instances of low ML/TF risk is acceptable.

Life insurance products are designed to financially protect the policyholder against the risk of an uncertain future event, such as death, illness or outliving savings in retirement. The protection is achieved by an insurer pooling the financial risks faced by many different policyholders. Life insurance products can also be bought as investment products or for pension purposes.

Life insurance products are provided through different distribution channels to customers who may be natural or legal persons or legal arrangements. The beneficiary of the contract may be the policyholder or a nominated or designated third party. Insurance intermediaries are important in the distribution, underwriting and claims settlement processes and are often the direct link to the policyholder. Under the strict conditions outlined in Section 3 of Part IV of this Guideline, an insurer may rely on the customer due diligence carried out by intermediaries such as agents and brokers, provided that the terms for such reliance are clearly outlined in the binding arrangement between the insurance company and its brokers and agents.

Most life assurance products are designed for the long-term and some will only pay out on a verifiable event, such as death or retirement. This means that many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial services products, there is a risk that the funds used to purchase the insurance product may be the proceeds from crime.

1. Risk Factors

In conducting its risk assessment consider the level of exposure faced by the business having regard to the following risk factors:

1.1 Product, Service and Transaction Risk Factors

The following factors may indicate higher risk:

i) flexibility of payments, for example the product allows:

- Payments from third parties;
- High value or unlimited value premium payments, overpayments or large volumes of lower value premium payments;
- Cash payments.

ii) The nature of the product such as unit-linked or non unit-linked single premium policies and annuities, as well as ease of access to accumulated funds, which allows

for high value lump sum payments, partial withdrawals or early surrender at any time, with limited charges or fees, make these types of products susceptible to money laundering risk.

iii) Negotiability, for example the product can be used as collateral for a loan.

iv) Acceptance of frequent payments outside of normal premium policy or payment schedule.

v) Risks arising from innovation. For example, new or developing technologies that facilitates or allows anonymity of the customer.

vi) The means and type of payment such as cash, wire transfer, third party cheque without any apparent connection with the prospective customer or beneficiary;

vii) Request for purchase of a policy requiring a large lump sum payment where the policyholder has previously requested only small, periodic-payment contracts;

viii) Attempts to use a third party cheque to make a purchase of a policy;

Where the product possesses the following characteristics it may indicate lower ML/TF risks:

The product:

i) Only pays out against a pre-defined event, for example death, or on a specific date, such as credit life insurance policies covering consumer and mortgage loans and paying out only on death of the insured person;

ii) Has no surrender value;

iii) Has no investment element;

iv) Has no third party payment facility;

v) Total investment is curtailed at a low value;

vi) Is a policy where the annual premium is no more than TTD 6,000 or consists of a single premium of no more than TTD 15,000;

vii) Only allows small value regular premium payments and no overpayment;

viii) Is accessible only through employers, for example a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;

ix) Cannot be redeemed in the short or medium term such as pension schemes;

x) Cannot be used as collateral;

xi) Does not allow cash payments.

1.2 Customer and Beneficiary Risk Factors

The following factors may indicate higher risk:

i) The nature of the customer, for example:

- Legal persons whose structure makes it difficult to identify the beneficial owner;

- The customer or the beneficial owner of the customer is a PEP;
- The beneficiary of the policy or the beneficial owner of this beneficiary is a PEP;
- The contract does not match the customer's wealth situation;
- The customer's profession or activities are regarded as particularly susceptible to money laundering for example because they are known to be very cash intensive such as casinos or exposed to high corruption risk; or exposed to terrorist financing risk such as remittance companies;
- The contract is subscribed by a 'gatekeeper' such as fiduciary financial institution, acting on behalf of the customer;
- The policyholder and/or the beneficiary of the contract are companies with nominee shareholders and/or shares in bearer form.

ii) The customer's behavior in relation to the insurance contract, for example:

- Frequent and unexplained surrenders, especially when the refund is done to different bank accounts;
- The customer makes frequent or unexpected use of 'free look' provisions/'cooling off' periods, in particular where the refund is made to an apparently unrelated third party;
- The customer incurs a high cost by seeking early termination of a product;
- The customer transfers the contract to an apparently unrelated third party;
- The customer requests change or increase of the sum insured and/or of the premium payment;
- Application for insurance outside the policyholder's normal pattern of business needs;
- Any lack of information or delay in the provision of information to enable verification to be completed;
- Any transaction involving an undisclosed party;
- Early termination of policy, especially at a loss caused by front end loading, or where cash was tendered and/or the refund cheque is to a third party;
- A transfer of the benefit of a policy to an apparently unrelated third party;
- Applicant shows no concern for the performance of the policy but much concern for its early cancellation provisions;
- Applicant is reluctant to provide normal information when applying for a policy, provides minimal or fictitious information, or provides information that is difficult or expensive to verify;
- Applicant appears to have an unusual number of policies with different insurers;

- Applicant purchases policies in amounts considered beyond the customer's apparent means;
- Applicant establishes a large insurance policy and within a short time period cancels the policy and requests that the cash value be paid to a third party;
- Applicant wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy;
- Applicant uses a mailing address outside the area where the application is made and where the home telephone is found to have been disconnected, upon verification attempt.

iii) In relation to the beneficiary:

- The insurer is being made aware of a change in beneficiary only when the claim is made;
- The customer changes the beneficiary clause and nominates an apparently unrelated third party.

iv) In relation to payments:

- Applicant attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments;
- Applicant requests to make a lump sum payment by a wire transfer or with foreign currency.
- The customer uses unusual payment methods, such as cash or structured monetary instruments or other forms of payment vehicles fostering anonymity;
- Payments from different bank accounts without explanation;
- Payments from banks which are not established in the customer's country of residence;
- The customer makes frequent or high value overpayments where this was not expected;
- Payments received from third parties that are not associated with the contract;
- Catch-up contribution to a retirement plan close to retirement date.

The following factors may indicate lower risk:

i) In case of corporate owned life insurance, the customer is:

- A credit or financial institution that is subject to requirements to combat money laundering and the financing of terrorism and supervised for compliance with these requirements in a manner that is consistent with the FOR;
- A public financial institution listed on a stock exchange and subject to regulatory disclosure requirements (either by stock exchange rules or through

law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a financial institution;

- A public administration or a public enterprise.

1.3 Distribution Channel Risk Factors

The following factors may indicate higher risk:

i) Non-face-to-face sales, such as online, postal or telephone sales, without additional safeguards;

ii) Long chains of intermediaries;

The following factors may indicate lower risk:

i) There are binding arrangements with intermediaries who are well known to the insurer, who is satisfied that the intermediary applies CDD measures commensurate to the risk associated with the relationship and in line with those required under the FOR;

ii) The product is only available to employees of certain companies that have a contract with the insurer to provide life insurance for their employees, for example as part of a benefits package.

1.4 Country or Geographic Risk Factors

The following factors may indicate higher risk:

i) The insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are in different jurisdictions;

ii) The insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are based in, or associated with, high risk jurisdictions, including those identified by the FATF, CFATF and FSRBs as countries with strategic deficiencies or to whom enhanced due diligence or counter-measures apply;

iii) Premiums are paid through accounts held with financial institutions established in high risk jurisdictions, including those identified by the FATF, CFATF and FSRBs as countries with strategic deficiencies or to whom enhanced due diligence or counter-measures apply;

iv) The intermediary is based in, or associated with, high risk jurisdictions, including those identified by the FATF, CFATF and FSRBs as countries with strategic deficiencies or to whom enhanced due diligence or counter-measures apply.

The following factors may indicate lower risk:

i) Countries are identified by credible sources such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems;

ii) Countries are identified by credible sources as having a low level of corruption, or other criminal activity.

2. Customer Due Diligence Measures

Part IV of the FOR stipulates specific CDD provisions for insurance companies and requires life insurers to apply CDD measures to the customer and beneficial owner and also to the beneficiaries as soon as they are identified or designated. This means that insurers must obtain:

i) The name of the beneficiary where either a natural or legal person or arrangement are identified as the beneficiary; or

ii) Sufficient information to be satisfied that the identity of the beneficiaries can be established at the time of payout where the beneficiaries are a class of persons or designated by certain characteristics. For example, where the beneficiary is 'my future grandchildren', the insurer could obtain information about the policyholder's children.

2.1 Verification of Identity

In principle, identification and verification of customers and beneficial owners should take place when the business relationship is established. Regulation 24(2) of the FOR however allows for verification requirements to be met after entering into an insurance contract provided certain criteria are met, including effective management of ML/TF risk. Regulation 29 of the FOR allows exceptions to verification of identity for certain types of insurance contracts.

In relation to beneficiaries, insurers must verify the beneficiaries' identities at the latest at the time of payout. Where the life insurance has been assigned to a third party who will receive the value of the policy, they must identify the beneficial owner at the time of the assignment.

In regard of policy surrenders, where such instances represent a one-off transaction or is conducted during the course of the business relationship and the value of the surrender is ninety thousand dollars or more, Regulation 28 of the FOR requires that the identity of the customer must be verified before the financial institution makes the payment to the customer.

2.2 Enhanced Due Diligence Measures

In addition to consideration of EDD measures (as appropriate) outlined in Part II of this Guideline, insurers should also consider:

i. Refunding the premium directly to the customer's bank account from which the funds were paid. Insurers must ensure that they have verified the customer's identity before making a refund, in particular where the premium is large or the circumstances appear otherwise unusual. Insurers must also consider whether the cancellation raises suspicions about the transaction and whether submitting a suspicious activity report to the FIU would be appropriate;

ii. Taking additional steps to strengthen the insurer's knowledge about the customer, the beneficial owner, the beneficiary or the beneficiary's beneficial owner, the third party payers and payees.

iii. If the payer is different from the customer, establishing the reason why;

iv. Where possible, identifying the beneficiary at the beginning of the business relationship, rather than wait until they are identified or designated;

v. Identifying and verifying the identity of the beneficiary's beneficial owner;

vi. In line with Regulation 27(6) of the FOR taking measures to determine whether the customer is a PEP and taking reasonable measures to determine whether the beneficiary or the beneficiary's beneficial owner is a PEP at the time of assignment, in whole or in part, of the policy or, at the latest, at the time of payout;

vii. Regulation 27(7) of the FOR also requires that where the risk associated with a PEP relationship is assessed as high, EDD must be conducted on the entire business relationship. Insurers must also inform senior management before the payout of the policy so that senior management can take an informed view of the ML/TF risk associated with the situation and decide on the most appropriate measures to mitigate that risk. Additionally, consideration must also be given to whether a suspicious activity report should be filed with the FIU.

2.3 Simplified Due Diligence

In line with Regulation 14(b), (c) and (d) of the FOR, insurers may apply simplified due diligence measures in relation to:

i. A pension fund plan, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deductions from wages and the pension fund plan rules do not permit assignment of the member's interest;

ii. Insurance policies for pension fund plans where there is no surrender clause and the policy cannot be used as collateral; and

iii. Where the annual premium is no more than six thousand dollars or consists of a single premium of no more than fifteen thousand dollars.

Notwithstanding the thresholds established in law, insurers may establish lower thresholds for the application of simplified measures that are commensurate with the size of transactions that are typically conducted at the institution. This should be applied on the basis of a comprehensive risk assessment to identify instances of lower risk based on the nature of the insurance financial institution. The rationale for the application of such simplified measures must be documented in the insurer's policies and procedures.

It should also be noted that the National Risk Assessment concluded that certain classes of insurance, namely general, health and term life, present low ML/TF risk. Additionally, the FATF Standards in respect of the insurance sector apply to the underwriting and placement of life insurance and other investment related insurance. In accordance with a risk based approach, the application of simplified due diligence in instances of low ML/TF risk is acceptable.

Simplified due diligence measures may for example be applied in instances of pure insurance covers which do not provide for payment of surrender values, such as hospital and surgical insurance, critical illness insurance and pure term life insurance covers. Additionally, for general insurance products

such as third party motor insurance with annual low premiums and less ML vulnerability, insurers may consider the application of simplified due diligence measures.

For reasons of sound business practice and proper risk management, insurers should already have controls in place to assess the risk associated with each policyholder. These existing controls are suitable not only for commercial risk assessment and fraud prevention but also mitigate against ML/TF risks. Reliance may be placed on existing controls to identify the customer and verification of identity may be at trigger events in the instances described below.

In low risk situations insurers may consider that verification of the identity:

i. **Of the customer** is fulfilled on the basis of a payment drawn on an account in the sole or joint name of the customer with regulated financial institution;

ii. **Of the beneficiary** of the contract is fulfilled on the basis of a payment made to an account in the beneficiary's name at a regulated financial institution.

2.4 Ongoing Due Diligence

In general, insurers should pay attention to all requested changes to the policy and /or the exercise of rights under the terms of the insurance contract. Generally in insurance, various transaction or trigger events occur after the contract date where due diligence will be applicable. These include claims notifications, surrender requests and policy alterations, including changes to benefits and beneficiaries.

A determination should be made if the change/transaction does not fit the profile of the customer and/or the beneficial owner or is for some reason unusual or suspicious.

Insurers may choose not to conduct further verification on previously conducted CDD in the following circumstances:

i. Renewal and reinstatement of policies with no significant changes to the term and conditions or the insurance policy (including benefits under the insurance policy); or

ii. Application of pure insurance covers which do not provide for payment of surrender values, such as hospital and surgical insurance, critical illness insurance and pure term life insurance covers.

2.5 Reliance on Intermediaries for CDD

Where reliance for CDD in placed on an intermediary, the provisions outlined in Part IV of this Guideline with respect to third party reliance applies. Insurers are reminded that the ultimate responsibility for knowing the customer or beneficiary always remains with the insurer. Insurers will therefore satisfy themselves as to the adequacy of CDD procedures conducted by insurance intermediaries on their behalf.

As noted in Section 3 of Part IV, where reliance is placed on an intermediary for due diligence, these arrangements must be governed in the terms of the Binding Agreement between the insurer and the broker or the agent. The insurer must be satisfied that they can immediately obtain the necessary information concerning the relevant identification data and other documentation pertaining to the

identity of the customer or beneficiary from the intermediary. The insurance intermediary must submit such information to the insurer upon request and without delay. Insurers must undertake and complete their own verification of the customer and beneficial owner if they have any doubts about the ability of the intermediary to undertake appropriate due diligence.

Insurers should consider refusing referred business from or terminating relationships with agents or brokers that do not comply with agreed upon client identification responsibilities or provide the insurer with the requisite client information on a timely basis.

Contracts with agents and brokers should be reviewed and updated as necessary to ensure compliance with the AML/ CFT laws and guidelines. The extent of the insurer's exposure to the agent or broker for the results of client due diligence should be addressed expressly in the insurer's business risk assessment.

C. SECTOR SPECIFIC GUIDANCE FOR MONEY REMITTERS

Money remittance business can be considered as the business of accepting cash, cheques, other monetary instruments or other stores of value in one location and the payment of a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money remitter belongs. Remittances may be domestic or international.

Remittances are integral to many economies across the region. They not only provide a stable source of income, but can increase financial inclusion, raise domestic tax revenues, and provide a vital source of external finance. At the same time, however, there is a general perception that the remittance sector is more vulnerable to ML/FT risks than other financial institutions. The nature of the service provided can expose money remitters to ML/TF risk. This is due to the simplicity and speed of transactions, their worldwide reach and often cash-based character. Since the events of 9/11, there have been increasing reports of the remittance sector being used to facilitate terrorist financing. As remittance volumes grow, so do concerns about potential risks.

Many money remitters use agents to provide payment services on their behalf. Agents often provide payment services as an ancillary component to their main business and they might not themselves be reporting entities under applicable AML/CFT legislation; accordingly, their AML/CFT expertise may be limited.

Having regard to the foregoing, money remitters like other financial institutions, are required to take reasonable steps to guard against money laundering and the financing of terrorism by assessing the risks and vulnerabilities associated with their operations and understanding and complying with AML/CFT requirements.

1. Risk Factors

1.1 Transaction or Service Risk

The risk associated with the transaction may vary depending on whether the money remitter is sending or receiving the transaction. An overall risk assessment should include a review of transactions as a whole. This should include a consideration of such factors as:

1.1.1 Transactions sent or attempted

i) Customer structures transaction in an apparent attempt to break up amounts to stay under any applicable threshold to avoid CDD requirements;

ii) Transaction is unnecessarily complex with no apparent business or lawful purpose;

iii) Number or value of transactions is inconsistent with financial standing or occupation, or is outside the normal course of business of the customer in light of the information provided by the customer at inception of the business relationship;

iv) Customer is willing to pay unusual fees to have transactions conducted;

v) Customer makes unusual inquiries, threatens or tries to convince employees to avoid providing CDD information;

vi) Customer sends money internationally and then expects to receive an equal incoming transfer or vice versa;

vii) Customer wires money to illegal online gambling sites; addresses containing gambling references or transfers to countries with large numbers of internet gambling sites;

viii) Customer is involved in transactions that have no apparent ties to the destination country and with no reasonable explanations;

ix) Customer wires money to higher-risk jurisdiction/country/corridor;

x) Customer attempts a transaction, but given that he would likely be subject to the CDD monitoring, cancels transaction to avoid reporting or other requirements;

xi) Transaction which are indicators of potential consumer fraud:

- Customer transfers money to claim lottery or prize winnings or to someone he or she met only online;
- Transfer towards credit card or loan fee or for employment opportunity or mystery shopping opportunity;

xii) Senders appear to have no familial relationship with the receiver and no explanation forthcoming for the transfer;

xiii) Activity detected during monitoring (in many of these scenarios the customer's activity may be apparent both during point-of-sale interaction and during back-end transaction monitoring);

xiv) Transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation;

xv) Unusually large aggregate wire transfers or high volume or frequency of transactions with no logical or apparent reason;

xvi) Customers whose concentration ratio of transfers made to a jurisdiction is notably higher than what is to be expected considering overall customer base;

xvii) A network of customers using shared contact information, such as address, telephone or e-mail, where such sharing is not normal or reasonable explicable.

1.1.2 Transactions received

Money remitters should pay special attention to:

i) Transactions that are not accompanied by the required originator or beneficiary information;

ii) When additional customer or transactional information has been requested from an ordering MVTS provider, but has not been received;

iii) Large number of transactions received at once or over a certain period of time which do not seem to match the recipient's usual past pattern;

iv) Multiple customers transfer funds to the same payee or appear to have the same identification information, e.g. address or telephone number.

1.2 Customer risk factors

The following factors may indicate higher risk in relation to the customer's business activity:

i) The customer owns or operates a business that handles large amounts of cash;

ii) Customer owns or operates a cash-based business that appears to be a front or shell financial institution or is intermingling illicit and licit proceeds as determined from a review of transactions that seem inconsistent with financial standing or occupation;

iii) The customer's business has a complicated ownership structure.

In relation to the nature of the customer or the customer's behaviour:

i) Customer who travels unexplained distances to locations to conduct transactions: the money remitter is not local to the customer or the customer's business;

ii) Evidence of customer networks; i.e. defined groups of individuals conducting transactions at single or multiple locations;

iii) The customer appears to be acting for someone else; for example others watch over the customer or stay visible outside, or the customer reads instructions from a note;

iv) The customer's behaviour makes no economic sense, for example the customer accepts a poor exchange rate or high charges unquestioningly or requests or provides large amounts of currency in either low or large denominations;

v) The customer's transactions stay just below applicable thresholds;

vi) The customer's use of the service is unusual, for example he sends or receives money to or from himself or sends funds on immediately after receiving them;

vii) The customer appears to know little or is reluctant to provide information about the payee;

viii) The customer is a PEP or the beneficial owner of a customer is a PEP;

ix) Non face-to-face customer, where doubts exist about the identity of such customer;

x) Customer who uses agents or associates where the nature of the relationship or transaction(s) makes it difficult to identify the beneficial owner of the funds;

xi) Customer knows little or is reluctant to disclose details about the payee (address/contact info, etc.);

xii) Consumer gives inconsistent information (e.g. provides different names);

xiii) Suspicion that the customer is acting on behalf of a third party but not disclosing that information or is being controlled by someone else (his/her handler). For example, the customer picks up a money transfer and immediately hands it to someone else or someone else speaks for the customer, but puts the transaction in his/her name;

xiv) Customer who has been the subject of law enforcement sanctions (in relation to proceeds generating crimes);

xv) Customer who offers false/fraudulent identification, whether evident from the document alone, from the document's lack of connection to the customer, or from

the document's context with other documents (e.g. use of identification cards or documents in different names without reasonable explanation);

xvi) Customer whose transactions and activities indicate connection with potential criminal involvement, typologies or red flags provided in reports.

The following factor may indicate lower risk:

i) The customer is a long-standing customer of the money remitter whose circumstances are known and understood and whose patterns of activity are consistent with the money remitter's knowledge of the customer. For example, the customer is known to be sending funds to their child studying abroad on a consistent basis.

1.3 Distribution channel risk factors

The following factors may indicate higher risk with respect to sub-agents. Sub-agents who:

i) Represent more than one money remittance principal;

ii) Have unusual turnover patterns compared to other agents in similar locations, e.g. unusually high transactions sizes, unusually large cash transactions, a high number of transactions that fall just under the CDD threshold , or undertake business outside normal business hours;

iii) Have transaction volume that is inconsistent with either overall or relative to typical past transaction volume;

iv) Have transaction patterns indicating predominance of transactions with values that are just beneath the CDD threshold;

v) Undertake a large proportion of business with payers or payees from high risk locations either domestically or internationally;

vi) Appear to be unsure about, or inconsistent in, the application of group-wide AML/CFT policies;

vii) Are located in a higher-risk location or serving high-risk customers or transactions;

viii) Are determined to be a PEP;

ix) Conduct an unusually high number of transactions with another agent location, particularly with an agent in a high risk geographic area or corridor;

x) That have been the subject of negative attention from credible media or law enforcement action;

xi) That have failed to attend or complete the training programs;

xii) That operate sub-standard compliance programs, i.e. programs that do not effectively manage compliance with internal policies, regulations and Guidelines;

xiii) Have a history of regulatory non-compliance and that are unwilling to follow compliance program review recommendations, and therefore subject to probation, suspension or termination;

xiv) Fail to provide required originator information upon request;

xv) Have data collection or record keeping that is lax, sloppy or inconsistent;

xvi) Appear willing to accept false identification or identification records that contain false information, non-existent addresses that would be known to be non-existent to a person in that area, or phone numbers that are used as fillers;

xvii) Have a send-to-receive ratio that is not balanced, consistent with other agents in the locale, or whose transactions and activities indicate potential complicity in criminal activity;

xviii) Have seasonal business fluctuation which is not consistent with their incomes or with other agents in the locale or is consistent with patterns of criminal proceeds;

xix) Have a ratio of questionable or anomalous customers to customers who are not in such groups that is out of the norm for comparable locations.

1.4 Country or Geographic Risk Factors

The following factors may indicate higher risk when payments are received from or sent to:

i) Countries/areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them;

ii) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling;

iii) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations organisation;

iv) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.

2. Customer Due Diligence Measures

Money remitters are required to conduct CDD on the customer, and where applicable, the beneficial owner and the person(s) acting on behalf of the customer when:

i) Establishing a business relationship;

ii) Conducting one-off or occasional transfers above TTD 6,000 where the transaction is carried out in a single operation or in several operations that appear to be linked;

iii) There is suspicion of ML/TF, regardless of the amount of the transaction;

iv) There is doubt about the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification;

v) When there is a change in risk-rating of the customer, or it is otherwise warranted by a change in circumstances of the customer.

2.1 Simplified Due Diligence

Simplified due diligence measures may be applied by a money remitter in relation to:

i) Instances defined in Regulation 14 of the FOR, including where lower risks have been identified through a national risk assessment or through an adequate assessment of risk by the money remitter;

ii) One-off wire transfers of TTD 6,000 or less, where the transaction is carried out in a single operation or in several operations that appear to be linked.

Notwithstanding the thresholds established in law, a money remitter may establish lower reporting thresholds that are commensurate with the size of transactions that are typically conducted, and as identified in their business risk assessment.

2.2 What constitutes a business relationship?

The business profile for a money remitter differs from that of a financial institution such as a bank or securities firm, in that the money remitter typically provides occasional, transaction-based services to walk-in customers and generally does not open or maintain accounts. However, some money remitters may introduce customer loyalty schemes and relationship management tools like membership cards that in effect constitute a business relationship.

A business relationship therefore in the context of a remittance service business is a business, professional or commercial relationship between the money remitter and a customer, which the business expects, on establishing the contact, to have an element of duration. For example, where there is a contract to provide regular services to a corporate customer or any other arrangement that facilitates an ongoing business relationship or repeat custom, such as providing a unique customer identification number or card for the customer.

2.3 Monitoring and Screening Systems and Processes

Since the nature of money remittance is primarily transaction-based with large number of customers involved and relatively small amounts transacted, it is imperative for money remitters to have adequate systems in place to collate relevant information and monitor customers' activities. Money remitters must have processes to detect and monitor transactions:

i) That indicate that an occasional transaction relationship has evolved into a business relationship (and any simplified occasional transaction concession would then be not applicable); and/or

ii) By customers who may be attempting to split large transactions into several smaller, less conspicuous amounts, which could indicate 'smurfing' or structuring i.e. linked transactions particularly in instances when the customer utilizes multiple locations to conduct transactions;

iii) From different customers that are destined for the same payee.

It is good practice to monitor for repeat business over the preceding three (3) months from the date of the most recent transactions, using risk indicators and profiles that are appropriate to the business.

Money remitters are also reminded of their obligations under Regulations 33 and 34 of the FOR to include relevant originator and beneficiary information on payment transfers and ensure that this information remains with the transfer throughout the payment chain.

The money remitter must also have processes to screen names of the sender and receiver and the destination country against designated sanctions lists and to have appropriate measures to identify where the customer is a PEP. EDD must be applied in accordance with Part II of this guidance where it is determined that a person is a higher riskPEP.

Where the risk factors associated with an occasional transaction or business relationship is elevated, money remitters should apply EDD in line with measures outlined in Part II, including, where appropriate, increased transaction monitoring (e.g. increased frequency or lower thresholds). Conversely, where the risk associated with an occasional transaction or business relationship is low and to the extent permitted by national legislation, money remitters may apply SDD measures in line with measures outlined in Part II.

2.4 Principal-Agent Relationships

Money remitters frequently enter into contractual arrangements with other parties to enable the remitter to provide services to customers by appointing an agent or sub-agent to act on behalf of the money remitter (the principal), to:

i) Accept money transmission instructions from customers;

ii) Undertake currency exchange; or

iii) Operate automated terminals for services such as bill payment terminals.

In a principal-agent relationship, the principal is the person who gives authority to an agent to act on the principal's behalf. However, the responsibilities of the principal do not absolve an agent from its legal obligations to comply with the AML/CFT requirements.

Typically, a written contract, an agency agreement between principal and agent is necessary to set out their respective roles and responsibilities. For example, an agency agreement may provide for the principal to give its agent access to technology, systems, forms, advertising and marketing material; and to written processes and procedures necessary to comply with the AML/CFT and other legal and regulatory requirements.

A principal should have a comprehensive and up-to-date agency agreement with each agent. It should maintain an up-to-date record of all the agents appointed in line with Regulation 31A of the FOR, including details of the shareholding structure, board of directors, management and locations of the agents.

An agency agreement should set out the obligations of the agent to comply with all the applicable AML/CFT and other legal and regulatory requirements, as well as the internal policies and procedures of the principal. The principal should ensure that the agent understands its responsibilities under the agency agreement.

The principal must establish strong oversight of its agents and be alert to any potential criminal activity by an agent, as well as the agent's customers. In accordance with Regulation 7(8) of the FOR,

the principal should put risk management controls in place, with clear accountability and adequate resources to support the oversight of agents.

In this regard the principal should consider the risk factors in relation to agents as outlined previously. Additionally, the principal should on a risk sensitive basis:

i) Carry out ongoing monitoring of customers and business transactions, including regular on-site visits to assess the compliance level as well as the effectiveness and adequacy of the agent's internal controls;

ii) Consider the nature and volume of an agent's business transactions as well as the agent's location to identify operations that are exposed to higher risk. These warrant more frequent on-site visits and more intensive monitoring;

iii) Ensure the agent flags suspicious transactions reports to the principal, for reporting to the FIU by the principal;

iv) Ensure that the agent refers to the principal for approval of:

- large value transactions based on thresholds set by the principal;
- transactions with PEPs and other high risk customers;

v) Ensure proper management of cash by the agent, including regular monitoring of cash holdings by the agent at its premises which should be in line with the nature, values and volume of transactions of the agent;

vi) Secure rapid corrective action to address any weaknesses that are identified, including where termination of an agency agreement is appropriate;

vii) Investigate cash holdings that exceed expected levels, or are inconsistent with the profile of transactions by the agent, to ensure that the agent is not involved in irregular activities.

2.4.1 Know Your Agent

Money remitters should know their agents. In this regard, money remitters should establish and maintain appropriate and risk-sensitive policies and procedures for their agents, including:

i. Obtaining evidence that the directors and other persons responsible for the management of the agent are fit and proper persons, taking into consideration their honesty, integrity and reputation;

ii. Taking reasonable measures to satisfy themselves that the agent's AML/CFT internal controls are appropriate and remain appropriate throughout the agency relationship, for example by monitoring a sample of the agent's transactions or reviewing the agent's controls on site;

iii. Providing AML/CFT training to agents to ensure that agents have an adequate understanding of relevant ML/TF risks and the quality of AML/CFT controls the money remitter expects.

D. SECTOR SPECIFIC GUIDANCE FOR BUREAUX DE CHANGE

In accordance with powers granted under Section 5 of the Exchange Control Act, Chapter 79:50, a bureau de change ('bureau') is authorized by the Central Bank to buy and sell foreign currency notes and coins only. A bureau can also buy but not sell travellers' cheques. This guidance is intended to provide practical guidance to a bureau in respect of CDD measures to be applied to its customers and must be read in conjunction with the general guidance provided in Part II of this Guideline.

Foreign exchange services are an important link in the money laundering chain particularly during the placement stage. Once the cash has been exchanged, it is difficult to trace its origin. Features of the bureau sector which makes it an attractive vehicle for laundering criminal funds include, the simplicity of foreign exchange transactions, the cash intensive character, low thresholds, the less than stringent customer identification procedures that are applied when compared with opening a bank account and reduced possibilities for verification of the customer's identification as with other financial institutions. The low frequency of contact can also be a significant vulnerability.

The provision of currency and the ability to convert currencies are the main areas of risk associated with bureau activities. Most customers, both personal and business, will have a legitimate need to convert currency. The risk is, however, failing to identify customers or situations where the level of foreign exchange activity is higher than one would expect, or is unusual or inconsistent in some way.

The nature of the relationship between a bureau and its respective customers can be fundamentally different from that established between other financial institutions and their customers. In this regard, there may be practical difficulties with implementing the full CDD requirements of the FOR. The nature and intended purpose of the majority of bureau transactions will be individuals requiring foreign currency for the purpose of business or leisure travel (or buybacks) and transactions typically will be small in value and occasional.

Bureaux are required to conduct a comprehensive ML/TF assessment in accordance with Part III of this Guideline. The risk assessment assists in developing the risk profile of customers that the bureau typically transacts with. In doing so, consideration should be given the character of its customers particularly in respect of it business locations. For example, customers transacting at bureau locations in the airport will be primarily members of the travelling public and foreign visitors compared to customers transacting at a non-airport bureau location. These may be primarily walk-in customers conducting small value transactions. In either situation, bureau employees must be alert to customers whose transactions are unusual in some way; who may be higher risk customers (for example, because they are nationals of a high risk country or may be a higher risk PEP); and whose activity or demeanor is unusual/suspicious in some way. The following are some questions to consider when developing the risk profile of the bureau customer:

i. The nature of the customer's interaction with the bureau, for example:
    - whether transactions are primarily one-off or occasional or repeat;
    - whether the customers are primarily the travelling public (i.e. tourists; vacationers or business travelers) or a non-travelling customer;

i. Whether the bureau is located in an area with highly transient customers;

ii. Whether the pattern of behaviour or changes to it, pose a risk;

iii. Whether customers are primarily individuals, companies or other type of non-individual customers;

iv. Whether a high percentage of customers are high risk such as PEPs;

v. Whether customers are based in high risk locations and jurisdictions.

The following risk factors may be considered when conducting the risk assessment:

1. Risk Factors

1.1 Transaction and Services Risks

The following may be indicators of higher risks:

i) Exchange of large quantities of low denomination notes for higher denominations;

ii) Exchange of large amounts or frequent exchanges that are not in line with the customer's business;

iii) Unusual/large cash transactions without a plausible or legitimate explanation;

iv) Frequent small transactions, which taken together are substantial;

v) Customers requesting information about threshold limits for transactions;

vi) Transactions that do not make commercial sense e.g. the customer is buying currency that does not fit with what the bureau knows of their travel destination;

vii) Split transactions: the more sophisticated money launderer will seek to split a large transaction into several smaller ones including structuring of transactions or smurfing to avoid transaction thresholds. Such splitting can occur within one location, or across several branches.

1.2 Customer Risk Factors

If unable to obtain a satisfactory explanation from the customer in the situations listed below, the bureau should treat this as an unusual activity:

i) The customer requests currency in large denomination notes;

ii) The customer buys currency that does not fit with what is known about the customer's destination;

iii) The customer buys currency from an unusual location in comparison to his/her own location;

iv) The customer apparently does not know the exact amount being exchanged;

v) The customer looks around all the time and does not observe the counting of money;

vi) The customer's behaviour makes no economic sense or is willing to accept very high or uncommercial penalties or charges or to accept poor rates of exchange;

vii) Frequent exchange of cash into various other currencies;

viii) The amounts exchanged are significantly higher than usual;

ix) There is no link between the amount of money exchanged and holiday periods;

x) High frequency of currency exchange transactions over a period of time;

xi) The customer is reluctant to provide normal information, or provides only minimal, false or misleading information;

xii) The customer is, or appears to be acting on behalf of another person, and there is an unwillingness to give the name of the person(s) they represent;

xiii) Situations where the source of funds cannot be easily verified or lack of adequate client identification (which the bureau may require for EDD or ongoing monitoring purposes);

xiv) Business customers who reluctant to provide complete information regarding the type of business, the purpose of the transaction, or any other information requested by the bureau.

In the event of an unusual activity, the bureau should conduct appropriate scrutiny of the activity, carry out EDD and in the event of a suspicion of ML/FT, an internal suspicious transaction report must be made to the CO. A determination should be made whether to refuse the transaction or terminate the business relationship with a repeat customer.

1.3 Distribution Channel Risks

i) Multiple bureau locations being used by the same customer within short periods;

ii) Unusual turnover patterns compared to other bureau locations and which do not make economic sense given the location: unusually high transactions volumes, unusually large cash transactions, a high number of transactions that fall just under the CDD threshold, or undertakes business outside normal business hours;

iii) The transaction volume of the location is inconsistent with either overall or relative to typical past transaction volume;

iv) Undertake a large proportion of business with customers from high risk locations either domestically or internationally;

v) Appear to be unsure about, or inconsistent in, the application of the AML/CFT policies.

The following are risk indications in relation to regular and existing customers of a bureau de change, without reasonable explanation for the changes:

i) The transaction is different from the normal business activity of the customer;

ii) The size and frequency of the transaction is different from the customer's normal pattern;

iii) The pattern has changed since the business relationship was established;

iv) There has been a significant or unexpected improvement in the customer's financial position.

2. Customer Due Diligence

Bureaux are required to conduct CDD on the customer, and where applicable, the beneficial owner and the person acting on behalf of the customer when:

i) Establishing a business relationship;

ii) There is suspicion of ML/TF, regardless of the amount of the transaction;

iii) There is doubt about the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification;

iv) When there is a change in risk-rating of the customer, or it is otherwise warranted by a change in circumstances of the customer.

Bureaux may conduct simplified due diligence as outlined in Regulation 14 of the FOR, including where lower risks have been identified through a national risk assessment or through an adequate assessment of risk by the Bureau itself.

Notwithstanding the thresholds established in law, a bureau may establish lower reporting thresholds that are commensurate with the size of transactions that are typically conducted and as identified in its business risk assessment.

A business relationship in the context of bureau business is a business, professional or commercial relationship between the bureau and a customer, which the business expects on establishing the contact, to have an element of duration. For example, where preferential rates are given to repeat customers or any other arrangement that facilitates an ongoing business relationship or repeat custom, such as providing a unique customer identification number for the customer. In such instances, the bureau must take steps to identify and verify the identity of the customer in accordance with Part IV of this Guideline.

It is acceptable for a bureau on the basis of its risk assessment to apply SDD measures or collect a reduced amount of identification information for certain types of customers and transactions which have been determined to pose lower risk, such as one-off or occasional transactions with members of the travelling public.

In lower risk instances, the customer's full name, date and place of birth, nationality and residential address and one form of identification may be obtained at a minimum. It is sufficient to simply understand and document the purpose of the customer's transaction. This can be based on a brief conversation/interaction with the customer or knowledge of the customer.

The customer's complete residential address must be recorded. Post Office box addresses are not acceptable. If a business address is being given as the official address of contact (where the applicant for business is a corporate customer) then the name of the business should also be given and the full business address stated. Descriptions such as "business place" will not be acceptable. If there is any uncertainty about the address, a contact number must be obtained from the customer. In line with a risk based approach, verification of address (for example, by obtaining a utility bill) and obtaining proof of income is not necessary for low risk customers conducting an occasional transaction.

2.1 Customers not resident in Trinidad and Tobago

The equivalent types of identity documents should be obtained for non-residents as for residents. If there are concerns that an identity document might not be genuine, contact the relevant embassy or consulate. Identification may also be verified using official documents such as job letters confirming employment arrangements for individuals on a work permit. Verification of address (for example, by

obtaining a utility bill) and obtaining proof of income is not necessary for lower risk customers conducting an occasional transaction.

Where higher ML/FT risk is identified, EDD must be carried out as appropriate. Bureaux should seek to document and verify additional information from customers where adverse or unusual factors give rise to suspicion.

In accordance with Part III of this Guideline, Bureaux must be able to demonstrate to the Central Bank that it has conducted a comprehensive risk assessment of the business and customers and on the basis of its assessment, implemented risk based CDD policies and procedures to allow employees to determine:

i. The risk profile of the customers;

ii. Where a customer and/or transaction pose a higher risk of ML/FT for example where the customer is a PEP;

iii. The appropriate level of customer diligence to be applied, for example to an international visitor compared to a repeat customer or a high risk customer.

3. Monitoring and Screening Processes

The bureau's CDD or KYC processes are therefore largely dependent on its ability to monitor and analyze transaction activity and customer behaviour. The bureau should have procedures, to identify and verify the identity of each customer who:

i. Conducts or attempts to conduct a transaction at or above the established monetary thresholds;

ii. Is a repeat customer and has an ongoing business relationship involving multiple transactions over a period of time with the bureau.

The bureau should also have appropriate measures to identify where the customer is a foreign PEP as well as reasonable measures to identify domestic and PEPs from international organizations. EDD must be applied in high risk instances in accordance with Parts II and IV of this Guideline, including obtaining approval for conducting the transaction; taking reasonable measures to establish the source of funds and wealth. The bureau's monitoring systems must facilitate ongoing enhanced monitoring where a business relationship is established with a PEP.

Where the bureau has a branch network these are issues to consider when developing the business risk profile:

i. Implementation of risk management procedures across the network of branches;

ii. Management and maintenance of records and type of records across the network;

iii. A monitoring system to identify where individuals or branches are not adhering to the risk management procedures;

iv. Ensure that all employees have been trained on the AML/CFT requirements and the bureau's procedures and are given ongoing training on recognising and dealing with suspicious transactions;

v. Ensure that all employees know who the CO is, are aware that the identity of the CO is not to be disclosed and are aware of the process for reporting unusual or suspicious activities and transactions.

3.1 Ongoing Monitoring

Some form of monitoring, whether it is automated, manual, a review of exception reports or a combination of several, depending on the risks presented, is required in order to detect unusual and hence possibly suspicious transactions. Even in the case of lower risk customers, a monitoring process is needed to verify that transactions match the initial low risk profile and if not, trigger an action to appropriately revise the customer's risk rating in accordance with Part III of this Guideline.

Bureaux should pay particular attention where the applicant for business is a corporate customer seeking to act through an agent/bearer (whether employed or contracted). An authorization letter should be obtained which clearly indicates the business to be transacted, that the agent/bearer is acting on the corporate customer's behalf and the bureau should ensure that the person signing to the letter is authorized to do so.

Where in relation to the corporate customer it appears to the bureau conducting the transaction, that the agent/bearer is not the usual agent/bearer, or the letter from the corporate customer is in any way defective, (e.g. it is not on official letterhead; there have been alterations or amendments to the contents of the letter, and/or these amendments are not signed in verification clearly by the author of the letter; or the letter itself is not signed) business should either not be transacted at all, or should be delayed until the corporate customer is contacted by the bureau and asked to confirm in writing or issue renewed written instructions and the confirmation or renewed instruction is in fact received. Even in the absence of these warning signals bureaux should, as a matter of course, employ the practice of conducting random checks with the corporate customer to satisfy itself of the genuineness and accuracy of the transaction to be conducted.

The minimum information that a bureau should obtain from its corporate customers are:-

i) Financial statements;

ii) Any changes to directors/principals/significant shareholders/ signing officers/ since the completion of the last corporate profile form;

iii) Main business to be carried out/services required by the customer;

iv) Purpose of foreign exchange activities the financial institution expects to conduct with the bureau e.g.:

- Business-related travel
- Importation of commercial goods;
- Investment activities;
- Other (details to be provided as to what the activity entails)

In outlining the purpose of the foreign exchange activities to be conducted, a general estimation of the frequency with which the financial institution expects to be conducting or actually conducts these

activities for the relevant period to be included e.g. daily; weekly; fortnightly; monthly; bi-monthly; quarterly; bi-yearly; annually; occasionally; or as the need arises.

E. SECTOR SPECIFIC GUIDANCE FOR TRUST COMPANIES

There appears to be limited potential for trusts to be used at the initial or placement stage of the money laundering process. Indeed, criminally derived funds would normally already have to have been inserted into the financial system before such assets could be placed into a trust. At the layering and integration stages of money laundering, however, there is greater potential for the misuse of trusts. Once the illegal proceeds have already entered the banking system, trusts could be exploited to further confuse the links between these proceeds and the illicit activity that generated them. The FATF have expressed concerns that this process may be even more effective if it is carried out in a number of countries and through legal professionals able to claim professional secrecy.

1. High Risk Trust Activities

1.1 Changes to Beneficiaries

Where all of the existing beneficiaries are removed and different beneficiaries are added, or where this is intended, or where the trust is intentionally structured to permit this. There may be perfectly legitimate reasons for this occurring or for this to be possible, but financial institutions should endeavour to ascertain what these are.

1.2 Unexplained Requests for Anonymity

Where the settlor's stated reason for establishing a trust is the need for anonymity or confidentiality in relation to himself or the beneficiaries. It should not be automatically inferred that this in itself is an illegitimate need. There are many instances where a settlor may desire that the extent or nature of his wealth is not known to third parties – such as children, the media, business or industry colleagues, potential kidnappers, industry competitors etc.

The legitimate need for privacy is acknowledged and supported and may be a reason for establishing a trust. However, financial institutions are encouraged to adopt a conservative and cautious approach in this area. In particular, where the reasons given by the settlor for the need for anonymity or confidentiality are not clear or are unconvincing, financial institutions should take appropriate further action.

1.3 Beneficiaries with no apparent connection to the settlor

Where there is no readily apparent connection or relationship of the settlor to the beneficiaries. Since the economic nature of a trust is a mechanism for the settlor to benefit a beneficiary, typically not in return for any consideration (payment, transfer of assets or provision of services), financial institutions should endeavour so far as possible to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom he seemingly has no connection. This can be a matter of great sensitivity (for example, where the beneficiary turns out to be an illegitimate child of the settlor) and financial institutions are encouraged to take this into account while pursuing necessary or appropriate inquiries.

1.4 Unexplained Urgency

Financial institutions are encouraged to inquire as to the reasons for any urgency, especially where the settlor is indicating that some of the due diligence process can or will be completed after the trust has

been established or a transaction has been entered into by the trustees or an underlying financial institution owned by the trust.

2. Customer Due Diligence

Financial institutions should make appropriate inquiry as to the source of the assets a settlor intends to settle. This will vary from case to case and depend on many factors, such as the type of trust intended to be created, the relative and absolute value of the assets intended to be settled, the objectives of the settlor in creating the trust and the timeframe within which the parties are working.

Financial institutions must recognize the need to adopt ongoing procedures in relation to trusts. In particular, each time assets are added to the trust by a new or existing settlor the same procedures should be followed.

Additional or successor trustees "step into the shoes" of the existing or predecessor trustees. A financial institution who is an additional or successor trustee should inquire of the existing or predecessor trustees whether appropriate inquiries were made of the settlor or settlors at the time of creating the trust and at the time of addition of any assets to the trust, and seek to obtain the originals or copies of the relevant due diligence documentation (e.g. verification of the settlor's identity and source of funds). Having done so, the financial institution should consider whether it is adequate, according to the circumstances of the particular case. However, in some cases such documentation may not be available or upon review may not be adequate. In such cases the financial institution should make reasonable inquiries of its own:

2.1 Where the Settlor is Dead

Where the settlor is alive, the financial institution should make the relevant inquiries of the settlor.

2.2 Where the Settlor is Dead

Where the settlor is dead, the financial institution should make reasonable inquiries about the settlor of such persons as may be appropriate in the circumstances of the particular case e.g. the existing or predecessor trustees or the beneficiaries. In particular, if the beneficiaries are relatives of the deceased settlor, as will often be the case, appropriate inquiry of the oldest beneficiaries may be the most fruitful.

APPENDICES

APPENDIX I -RISK INDICATORS FOR TERRORIST FINANCING

1. Financial and Behavioural Indicators[79]

1.1 Indicators linked to the financial transactions:

- The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
- The transaction is not economically justified considering the account holder's business or profession.
- A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
- Transactions which are inconsistent with the account's normal activity.
- Deposits were structured below the reporting requirements to avoid detection.
- Multiple cash deposits and withdrawals with suspicious references.
- Frequent domestic and international ATM activity.
- No business rationale or economic justification for the transaction.
- Unusual cash activity in foreign bank accounts.
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
- Use of multiple, foreign bank accounts.

1.2 Behavioral Indicators:

- The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
- Use of false corporations, including shell-companies.
- Inclusion of the individual in the United Nations 1267 Sanctions list.
- Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
- Beneficial owner of the account not properly identified.
- Use of nominees, trusts, family member or third party accounts.
- Use of false identification.

[79] Source: Egmont

2. Potentially Suspicious Activity That May Indicate Terrorist Financing[80]

2.1 Activity Inconsistent with the Customer's Business:

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as noncooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

2.2 Funds Transfers:

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

2.3 Other Transactions That Appear Unusual or Suspicious:

[80] Source:FFIEC BSA/AML Examination Manual

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.
- Banks from higher-risk locations open accounts.
- Funds are sent or received via international transfers from or to higher-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

3. Financial Red Flags[81]

- IP logins in areas of conflict such as near the Syrian border, to include Jordan and Lebanon, but particularly in Turkey
- Periods of transaction dormancy, which could be the result of terrorist training or engagement in combat
- ATM cash withdrawals in areas of conflict
- Wire transfers to areas of conflict
- Charitable activity in areas of conflict especially in Syria
- Financial activity identifiable with travel [purchase of airline tickets] to Syria through Turkey and other points of entry to include Jordan, Lebanon and Israel

4. Terrorist Activity Financing Related Indicators[82]

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) noted that a single indicator on its own may seem insignificant, but combined with others, could provide reasonable grounds to suspect that the transaction is related to terrorist financing activity.

- Client accesses accounts, and/or uses debit or credit cards in high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Client identified by media or law enforcement as having travelled, attempted/intended to travel to high risk jurisdictions (including cities or districts

[81] Source: **DML Associates LLC.** Dennis Lormel, founder and president of DML Associates, LLC, established and directed the FBI's terrorist financing initiative following the terrorist attacks of September 11, 2001.
[82] Source: FINTRAC

of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.

- Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- The client mentions that they will be travelling to, are currently in, or have returned from, a high risk jurisdiction (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Client depletes account(s) by way of cash withdrawal.
- Client or account activity indicates the sale of personal property/possessions.
- Individual/Entity's online presence supports violent extremism or radicalization.
- Client indicates planned cease date to account activity.
- Client utters threats of violence that could be of concern to National Security/Public Safety.
- Sudden settlement of debt(s) or payments of debts by unrelated 3rd party(ies).
- Law enforcement indicates to reporting entity that the individual/entity may be relevant to a law enforcement and/or national security investigation.
- Client's transactions involve individual(s)/entity(ies) identified by media or law enforcement as the subject of a terrorist financing or national security investigation.
- Client donates to a cause that is subject to derogatory publicly available information (crowdfunding initiative, charity, NPO, NGO, etc.).
- Client conducts uncharacteristic purchases (e.g. camping/outdoor equipment, weapons, ammonium nitrate, hydrogen peroxide, acetone, propane, etc.).
- A large number of email transfers between client and unrelated 3rd party(ies).
- Client provides multiple variations of name, address, phone number or additional identifiers.
- The sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity.

APPENDIX II – PEP IDENTIFICATION SOURCES

EXAMPLES OF INSTITUTIONS ESTABLISHED BY REGIONAL AND INTERNATIONAL ORGANIZATIONS

Caribbean Community and Common Market (Established by the Treaty of Chaguaramas)

Association of Caribbean States (ACS) (Established by the Convention Establishing the Association of Caribbean States)

Development Bank of Latin America (Established by Agreement Establishing Corporación Andina de Fomento)

Caribbean Agricultural Health and Food Safety Agency (Established by the Agreement Establishing the Caribbean Agricultural Health and Food Safety Agency)

Caribbean Aviation Safety and Securing Oversight System (Established by the Agreement Establishing the Caribbean Aviation Safety and Securing Oversight System)

Caribbean Centre for Development Administration (Established by the Agreement Establishing the Caribbean Sub-centre of the Latin American Centre for Development Administration)

Caribbean Community Implementation Agency for Crime and Security (Established by the Agreement Establishing the Caribbean Community Implementation Agency for Crime and Security)

Caribbean Court of Justice (Established by the Agreement Establishing the Caribbean Court of Justice)

Caribbean Court of Justice Trust Fund (Established by the Agreement Establishing the Caribbean Court of Justice Trust Fund)

Caribbean Disaster Emergency Management Agency (Established by the Agreement Establishing the Caribbean Disaster Emergency Response Agency)

Caribbean Examinations Council (Established by the Agreement Establishing the Caribbean Examinations Council)

Caribbean Regional Fisheries Mechanism (Established by the Agreement Establishing the Caribbean Regional Fisheries Mechanism)

Caribbean Meteorological Organisation (Established by the Agreement Establishing the Caribbean Meteorological Organisation)

Caribbean Public Health Agency (Established by the Agreement Establishing the Caribbean Public Health Agency)

Organisation of Eastern Caribbean States (Established by the Treaty of Basseterre Establishing the Organisation of Eastern Caribbean States)

Eastern Caribbean Supreme Court (ECSC) (Established by the West Indies Supreme Court Order)

Eastern Caribbean Central Bank (Established by the Agreement Establishing the Eastern Caribbean Central Bank)

Eastern Caribbean Civil Aviation Authority (Established by the Agreement Establishing the Eastern Caribbean Civil Aviation Authority)

Eastern Caribbean Telecommunications Authority (Established by the Agreement Establishing the Eastern Caribbean Telecommunications Authority)

Community of Latin American and Caribbean States (Established by the Declaration of Caracas creating CELAC)

Union of South American Nations (Established by the Constitutive Treaty of the Union of South American Nations)

Sistema de la Integración Centroamericana (Established by the Tegucigalpa Protocolo)

United Nations Economic Commission for Latin America and the Caribbean (Established by the established by Economic and Social Council resolution 106(VI) of 25 February 1948)

Amazon Cooperation Treaty Organization (Established by the Amazon Cooperation Treaty)

Pan American Health Organization (Established by the International Sanitary Convention of the American Republics)

Inter-American Court of Human Rights (Established by the American Convention on Human Rights)

Inter-American Institute for Cooperation on Agriculture (Established by the Convention on the Inter-American Institute for Cooperation on Agriculture)

El Sistema Económico Latinoamericano y del Caribe (Established by the Panama Convention Establishing the Latin American Economic System (SELA))

Asociación Latinoamericana de Integración (Established by the Treaty of Montevideo)

MERCOSUR (Established by the Treaty Establishing a Common Market with the Republic of Argentina, Federative Republic of Brazil, Republic of Paraguay and the Oriental Republic of Uruguay (Treaty of Asunción))

Latin American and Caribbean Parliament (Established by the Treaty of the Latin American Parliament)

Comunidad Andina (Established by the Andean Subregional Integration Agreement (Cartagena Agreement))

International

African Development Bank Group (Established by the Agreement Establishing the African Development Bank)

Arctic Council (Established by the Declaration on the Establishment of the Arctic Council)

Asian Development Bank (Established by the Agreement Establishing the Asian Development Bank – ADB Charter)

Association of Southeast Asian Nations (ASEAN) (Established by the Asean Declaration)

Bank for International Settlements (Established by the Constituent Charter of the Bank for International Settlements)

Basel Committee on Banking Supervision (Established by the Basel Committee on Banking Supervision Charter)

Caribbean Development Bank (Established by the Agreement Establishing the Caribbean Development Bank)

Commonwealth (Established by the Balfour Declaration, Statute of Westminster and London Declaration)

Community of Democracies (Warsaw Declaration)

Council of Europe (Established by the European Convention on Human Rights)

European Bank for Reconstruction and Development (Established by the Agreement Establishing the European Bank for Reconstruction and Development)

European Free Trade Association Secretariat (Established by the European Free Trade Agreement Convention)

European Space Agency (Established by the Convention for the establishment of a European Space Agency)

Inter-American Development Bank (IDB) (Established by the Agreement Establishing the Inter-American Development Bank)

International Criminal Court (Established by the Rome Statute of the International Criminal Court)

International Commission of Missing Persons (Established by the Agreement on the status and functions of the International Commission on Missing Persons)

International Criminal Police Organization (Established by the Constitution of the ICPO-INTERPOL)

International Energy Agency (Established by the Agreement on an International Energy Program)

International Energy Forum (Established by the International Energy Forum Charter)

International Joint Commission (Established by the Boundary Waters Treaty)

International Mobile Satellite Organization (Established by the Convention on the International Maritime Satellite Organization)

International Organization for Migration (Established by the Constitution of the Intergovernmental Committee for European Migration)

International Seabed Authority (Established by the United Nations Convention on the Law of the Sea)

International Telecommunications Satellite Organization (Established by the Agreement relating to the International Telecommunications Satellite Organization)

International Union for Conservation of Nature (Established by the formal act of 1948 constituting the International Union for Protection of Nature)

La Francophonie (Established by the l'Agence de Coopération Culturelle et Technique (ACCT) Convention)

North Atlantic Treaty Organization (NATO) (Established by the North Atlantic Treaty)

Organization for Economic Co-operation and Development (Established by the Organisation for Economic Co-operation and Development Convention)

Organization for Security and Co-operation in Europe (Established by the Helsinki Final Act)

Organization of American States (Established by the Charter of the Organization of American States)

Permanent Court of Arbitration (Established under Article 20 of the 1899 Hague Convention for the Pacific Settlement of International Disputes)

United Nations (Established by the Charter of the United Nations)

- Food and Agriculture Organization of the United Nations (Established by the Constitution of the Food and Agriculture Organization)
- International Civil Aviation Organization (Established by the Convention on International Civil Aviation)
- International Labour Organization (Established by International Labour Organization Constitution)
- International Maritime Organization (Established by the Convention on the International Maritime Organization)
- International Monetary Fund (Established by the Articles of Agreement of the International Monetary Fund)

- International Telecommunication Union (Established by the International Telegraph Convention. However, in 1934 the International Telegraph Convention of 1865 was then combined with the International Radiotelegraph Convention of 1906 to form the International Telecommunication Convention.)
- United Nations Educational, Scientific and Cultural Organization (UNESCO) (Established by the Constitution of UNESCO)
- World Bank Group (Established by the Bretton Woods agreements)
- World Customs Organization (Established by the Convention establishing a Customs Co-operation Council)
- World Health Organization (Established by the constitution of the World Health Organization)
- World Intellectual Property Organization (Established by the Convention Establishing the World Intellectual Property Organization)
- World Meteorological Organization (Established by the World Meteorological Convention)
- World Tourism Organization (Established by the Statutes of the World Tourism Organization)
- Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization (Established by the Comprehensive Nuclear-Test-Ban Treaty)
- International Atomic Energy Agency (Established by the Statute of the International Atomic Energy Agency)
- Organisation for the Prohibition of Chemical Weapons (Established by the Chemical Weapons Convention)
- World Trade Organization (Established by the Marrakesh Agreement)

The Association of Southeast Asian Nations (ASEAN) established the:

- Economic Research Institute for ASEAN and East Asia (ERIA) established by the adoption of the formal statement agreed to at the 3rd East Asia Summit in Singapore

The North Atlantic Treaty Organization (NATO) established the:

- NATO Communication and Information Agency (NCI Agency) established by the NCIO Charter, which transferred and amalgamated the functions of various agencies into the NCI Agency
- NATO Support and Procurement Organization (NSPO) established by the NSPO Charter, which merged the names and roles of two NATO agencies into NSPO

REFERENCES

Basel Committee on Banking Supervisors (2016), Guidelines *Sound Management of Risks related to Money Laundering and Financing of Terrorism*

FATF (2016), *Guidance Correspondent Banking Services*, Paris, France

FATF (2016), *Guidance for a Risk Based Approach for Money or Value Transfer Services*, Paris, France

FATF (2015a), *Financing of the Terrorist Organisation of the Islamic State and the Levant (ISIL),* (the 'FATF ISIL report'), FATF, Paris France

FATF (2015b), *Guidance to a Risk-Based Approach to Virtual Currencies*, FATF, Paris, France

FATF (2014a), *Risk of terrorist abuse in non-profit organisations* (the "NPO report'), Paris, France

FATF (2014), *Guidance Risk-Based Approach for the Banking Sector* Paris, France

FATF (2013), *Guidance on Politically Exposed Persons (Recommendations 12 and 22)*, Paris, France

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, *updated June 2017*,Paris, France

FATF (2012), *Specific Risk Factors in the Laundering of Proceeds of Corruption,* FATF, Paris

FATF (2012), *Guidance Anti-money laundering and terrorist financing measures and financial inclusion*

FATF (2010), *Money Laundering Using New Payment Methods*, FATF, Paris,

Federal Financial Institutions Examination Council, BSA/AML Manual https://www.ffiec.gov/

Office of the Comptroller of the Currency, *Supervisory Guidance on Model Risk Management*, April 2011

The Wolfsberg Group (2017) *Guidance on Politically Exposed Persons (PEPs)*

CENTRAL BANK OF
TRINIDAD & TOBAGO