Version no:	1.1
Date Prepared:	04/11/2025
Date Revised:	02/03/2026

GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT OF TRINIDAD AND TOBAGO
Ministry of Finance

adopting a Risk Based Approach to AML/CFT/CPF

Purpose

This Guidance is intended to provide assistance to Non-Regulated Financial Institutions and Listed Businesses (collectively "Supervised Entities") on the conduct of an institutional AML/CFT/CPF Risk Assessment and the implementation of a Risk Based Approach to AML/CFT/CPF

Published 4 November, 2025
FIUTT REFERENCE: GN/005/2025

Version no: 1.1
Date Prepared: 04/11/2025
Date Revised: 02/03/2026

Table of Contents

Version no: 1.1
Date Prepared: 04/11/2025
Date Revised: 02/03/2026

VERSION	DATE	AUTHOR	DESCRIPTION	APPROVED BY	STATUS
1.0	04/11/2025	Legal Division	GN/005/2025 Approved Final Version	Director FIUTT	Final
1.1	25/02/2026	Legal Officer I	Part 3 was revised to reflect amendments made to the Financial Obligations Regulations, 2010 incorporating VASP obligations.	Director FIUTT	Final

1. Introduction and Purpose

1.1 This Guidance Note is issued to support Non-Regulated Financial Institutions and Listed Businesses ("Supervised Entities") in Trinidad and Tobago in fulfilling their obligations under Regulations 7 and 14(2) of the Financial Obligations Regulations 2010, ("FORs"), which mandates the adoption of a Risk-Based Approach ("RBA") to Anti-Money Laundering, Counter Financing of Terrorism and Counter Proliferation Financing ("AML/CFT/CPF") compliance. Supervised Entities are required to identify, assess, understand, and document their Money Laundering, Terrorist Financing and Proliferation Financing ("ML/TF/PF") risks and implement proportionate controls.

1.2 This Note also aligns with the Financial Action Task Force ("FATF") Recommendation 1, which requires countries and Supervised Entities to base their AML/CFT/CPF strategies on a comprehensive understanding of risk. The guidance is informed by the findings of Trinidad and Tobago's Second National Risk Assessment ("NRA2"), which provides sector-specific insights into vulnerabilities and threats. Supervised Entities should familiarise themselves with the NRA2 and any trends and typology reports issued by the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT") and other Competent Authorities, when applying a RBA. Supervised Entities are expected to integrate these findings into their institutional risk assessments and compliance programmes.

1.3 Supervised Entities should also be aware of the relevant requirements of the FATF 40 Recommendations, which have an impact on their operations and keep abreast of developments in the ML/TF/PF landscape, including changes in domestic AML/CFT/CPF laws, which can affect their understanding of risk.

1.4 **Advantages of implementing a Risk-Based Approach** - An effective RBA enables Supervised Entities to apply informed judgment in fulfilling AML/CFT/CPF obligations by implementing appropriate measures aligned with identified risks. The RBA does not restrict Supervised Entities to low-risk transactions or customers. Instead, it supports effective management of ML/TF/PF risks by enabling the strategic allocation of resources based on risk prioritisation.

2. Understanding AML/CFT/CPF Risks

2.1 AML/CFT/CPF risks refer to the potential for a Supervised Entity to be exploited for ML/TF/PF. These risks can arise from various sources, including the nature of the Supervised Entity's customers, the products and services offered, the delivery channels used, and the geographic areas in which the Supervised Entity operates. For example, customers who are politically exposed persons (PEPs), non-residents, or those operating in cash-intensive sectors may present higher risks. Similarly, products such as trust and company services, high-value goods, or anonymous transactions can be more vulnerable to misuse. Delivery channels like online platforms or third-party agents may obscure the origin of funds, while geographic exposure to FATF identified high-risk jurisdictions increases the likelihood of cross-border financial crime. Supervised Entities must understand how these factors interact and compound to form their overall risk profile.

2.2 NRA2 identifies drug trafficking, corruption, fraud, illicit arms trafficking and human trafficking as being the highest ML threats in Trinidad and Tobago. The Gaming Houses/Pool Betting sector was rated as having high vulnerability, while Real Estate, Private Members Clubs, and Money Value Transfer Services were assessed as medium-high vulnerability sectors.

(Please refer to NRA2 for further information on the ML/FT Threats and Vulnerabilities of Trinidad and Tobago).

3. Establishing a Risk Assessment Framework

3.1 In accordance with Regulation 7(2) of the FORs, Supervised Entities must establish a structured framework for risk assessment, comprising four key steps:

Step 1: Risk Identification

3.1.1 Supervised Entities should begin by identifying all relevant ML/TF/PF risk factors. This includes analysing customer types (e.g., individuals, legal persons, trusts), products and services (e.g., loans, real estate transactions, company formation), delivery channels (e.g., face-to-face, online), and geographic locations (e.g. jurisdictions listed by FATF as high-risk). Internal data such as transaction history, customer complaints, and audit findings should be used alongside external sources like FIUTT advisories, NRA findings, and FATF typologies.

3.1.2 In accordance with regulation 23 of the FORs, Supervised Entities should also identify and assess the ML/TF/PF risks of new products, new business practices, including new delivery mechanisms, as well as the use of new technologies for both new and existing products and services, such as virtual assets or new payment technologies. ***This Risk Assessment Framework should also be utilised prior to the implementation of such new products, services or technologies so that the SE is able to determine the potential impact of ML/TF/PF risks before use.***

3.1.3 The following Regulations were implemented to facilitate the Risk Assessment Framework for virtual assets. These regulations are applicable to you if you are a Supervised Entity who conducts business with or on behalf of a Virtual Asset Service Provider ("VASP"). If you are a Supervised Entity who is also registered with the Trinidad and Tobago Securities and Exchange Commission ("TTSEC") to conduct the business of a VASP, please refer to the Guidance issued by the TTSEC for your VASP business -

- *In accordance with regulation 38G of the FORs, where there is a transfer of virtual assets being conducted with missing or incomplete information about the originator, a beneficiary virtual asset service provider shall adopt risk-based policies and procedures for determining whether to execute, reject or suspend a transfer of virtual assets and the resulting procedures to be applied where the required originator or beneficiary information is incomplete.*
- *Further, regulation 38J provides that an intermediary virtual asset service provider shall take reasonable measures which are consistent with straight through processing, to identify transfer of virtual assets that lack required originator or beneficiary information and adopt risk-based policies and procedures for determining when to execute, reject or suspend a transfer of assets and the resulting procedures to be applied where the required originator or beneficiary information is incomplete.*
- *Regulation 38N provides that an intermediary virtual asset service provider shall have risk-based policies and procedures for determining when to execute, reject, or suspend a transfer of virtual assets lacking required originator or required beneficiary information and the appropriate follow-up action.*
- *In accordance with Regulation 38O, where a financial institution sends or receives a transfer of virtual assets on behalf of a customer, the financial institution shall be subject to the same obligations, including- the collection, verification, transmission, and protection of originator and beneficiary information and the application of a risk-based approach and the record keeping requirements.*

3.1.4 When identifying PF risks, Supervised Entities should have regard to the Supervised Entity's potential for:

- Non-implementation of targeted financial sanctions in relation to proliferation financing;
- Breach of targeted financial sanctions in relation to proliferation financing; and
- Evasion of targeted financial sanctions in relation to proliferation financing.

Supervised Entities should consult the FIUTT's Guidance to a Risk Based Approach for Counter-Proliferation Financing for Reporting Entities for further information.

3.1.5 The vulnerability of a business to ML/TF/PF is influenced by its size and operational complexity. Therefore, potential risks will vary across Supervised Entities. Businesses which engage in complex, cross-border transactions may present more opportunities for illicit financial activity compared to those operating solely within domestic boundaries, smaller structures and no or limited high risk customers.

Step 2: Risk Assessment and Evaluation

3.1.6 Once risks are identified, Supervised Entities must assess the likelihood and potential impact of each risk. This involves assigning risk ratings (e.g., low, medium, high) based on qualitative and quantitative criteria. For example, a customer from a high-risk jurisdiction conducting large cash transactions may be rated as high risk; or the service of forming trusts for foreign clients as offered by a legal practitioner or a trust and company service provider, may be rated high-risk due to potential misuse for asset concealment. Supervised Entities should use risk matrices or scoring models to ensure consistency and objectivity.

Risk Matrices or Scoring Models

The Risk Matrix or Scoring Model presents a visual representation of the likelihood and potential impact of each risk. ***Likelihood x Impact = Risk Level***

- ***<u>Likelihood:</u>***

Likelihood refers to the potential of a particular risk occurring. A Supervised Entity should use the possible risk factors and events, which have been identified under step 1, and determine the likelihood of an occurrence of each factor or event identified. The following are three examples which can be used to represent the likelihood of risk levels, however, based on each Supervised Entity's individual business model, this scale may be adjusted to accommodate more nuanced levels:

(a) ***Very Likely***: Almost certain – it will probably occur several times a year
(b) ***Likely:*** High probability it will happen once a year
(c) ***Unlikely:*** Not likely to occur, but also not impossible

- ***<u>Impact:</u>***

Impact refers to the seriousness of the damage, which would occur should the risk occur. The Supervised Entity should be cognisant of the negative effects to its business if the risk events were to occur, and assign a corresponding impact level. Some relevant impacts to consider would include, *but are not limited to*: financial loss, data loss, reputational loss, regulatory non-compliance and litigation. The following are examples of impact levels, however, similar to the risk levels, this scale may be adjusted to accommodate more nuanced levels depending on the Supervised Entity's individual business model:

(a) ***Major:*** Severe damage
(b) ***Moderate***: Moderate level of damage
(c) ***Minor:*** Minimal damage.

- ***Risk Matrix and Risk Score:***

After assessing the likelihood and impact of each risk, the level of risk will be determined based on the combination of these two factors. A risk matrix can be used to present a visualisation of this combination and to obtain a final risk score, which should then be used to assist the Supervised Entity in determining what actions should be taken to mitigate overall risks. A sample Risk Matrix and Risk Scoring Model is provided at **Appendix I** for example purposes only.

Risk matrices will differ depending on the nature and operations of each Supervised Entity and it is not expected that all Supervised Entities will implement the same Risk Matrix and Scoring model.

3.1.7 The results of the risk assessment should be documented in a formal Risk Assessment Report, which must be approved by senior management and reviewed periodically. Equally, there should be a mechanism to make the results of the risk assessment report available to the FIUTT as the Supervisory Authority.

Step 3: Risk Mitigation

3.1.8 For each identified risk, Supervised Entities must implement appropriate controls. Controls refer to the programmes, policies, and procedures established by Supervised Entities, and documented in the Compliance Programme, to prevent the occurrence of ML/TF/PF risks or to detect and report them early. These measures help ensure ongoing compliance with regulatory requirements governing the Supervised Entity's operations.

3.1.9 These may include enhanced due diligence ("EDD") for high-risk customers, transaction monitoring systems, staff training on red flags and reporting, and internal audit procedures. Controls should be proportionate to the level of risk and designed to prevent, detect, and respond to suspicious activity. For example, EDD may involve verifying the source of funds, conducting background checks, and obtaining senior management approval for on-boarding.

Step 4: Monitoring and Review

3.1.10 Risk assessments must be dynamic and responsive to changes in the business environment. The method applied to assess risks can be used for as long as it is suited to the business type and is tailored to the NRA and other typologies and risk assessments published in the local context.

3.1.11 Supervised Entities should establish procedures for ongoing monitoring of risk indicators, such as changes in customer behaviour or regulatory updates. Independent testing of the AML/CFT/CPF programme should be conducted periodically to ensure effectiveness. The risk assessment should be reviewed at least annually or when significant changes occur (e.g., new products or services offered, expansion into new markets or new customer bases).

4. Implementing a Risk-Based Approach

4.1 The RBA enables Supervised Entities to tailor their AML/CFT/CPF measures to the specific risks they face. Upon the identification and assessment of ML/TF/PF risks, these risks should be ranked by severity. The Supervised Entity should develop and implement mitigating controls, which are adequate and proportionate to the risks identified and ensure the effective alignment of its policies with the NRA and other sectoral risk assessments. This alignment fosters consistency across the financial and listed businesses sectors and enhances the nation's overall ability to combat ML/TF/PF.

Proportionate mitigating controls

4.2 Rather than applying uniform controls across all customers and transactions, the RBA allows for differentiated treatment based on risk levels. High-risk customers may require EDD, frequent monitoring, and senior management oversight, while low-risk customers may be subject to simplified due diligence ("SDD"). The RBA also helps Supervised Entities avoid unnecessary de-risking, which can exclude legitimate customers from access to financial and other services. To implement the RBA effectively, Supervised Entities must ensure that staff are trained to recognise risk indicators and apply controls consistently. Policies and procedures should clearly define risk categories, mitigation strategies, and escalation protocols. Supervised Entities should ensure that proportionate mitigating measures are applied to changes in risks, including new and emerging risks to its business.

4.3 See the FIUTT's Customer Due Diligence Guidance to Supervised Entities for further information on the implementation of EDD and SDD in the Customer Due Diligence ("CDD") Process, as well as the FIUTT's Guidance to Supervised Entities when conducting Business with Politically Exposed Persons.

5. Integrating Risk Assessment into the Compliance Programme

5.1 The AML/CFT/CPF compliance programme must be built around the findings of the Supervised Entity's risk assessment. Governance structures should ensure that senior management is actively involved in risk oversight and decision-making. Policies should cover CDD, EDD, SDD, ongoing monitoring, suspicious transaction reporting ("STR"), record keeping, ongoing training, independent testing, the compliance officer's roles and responsibilities, beneficial ownership, know your employees' policies and group policies.

5.2 Supervised Entities must also implement procedures for complying with Targeted Financial Sanctions (TFS), including screening against UN and domestic sanctions lists for TF and PF. ***It should be noted that the requirements for screening and freezing are mandatory and not risk based.*** See the FIUTT's Guidance on the procedures for Reporting Terrorist Funds, and the RBA to Counter-Proliferation Financing Risks – A Best Practices Paper, for further guidance.

5.3 Supervised Entities must ensure that their compliance programmes are documented, approved by senior management, and independently tested. More guidance on the creation and maintenance of a Compliance Programme can be read in the FIUTT's Guidance to NRFIs and LBs on how to structure an AML/CFT/CPF Compliance Programme.

5.4 Internal and independent audits should assess the effectiveness of controls and recommend improvements. For more guidance on conducting independent testing of the Compliance Programme, please consult the FIUTT's Guidance on Independent Testing for NRFIs and LBs.

5.5 The Supervised Entity should also ensure that its training programme is tailored to its risk profile and include case studies, typologies, regulatory updates and NRA findings.

5.6 Compliance Programmes should be reviewed and updated, as applicable, whenever there has been a change in risks and applicable legislation. This ensures that risk mitigation measures remain in line with risks identified and that all relevant employees are aware of the most up to date measures to be taken to reduce any negative impacts on the Supervised Entity's business.

6. Sector-Specific Examples

Listed Businesses

6.1 *Real Estate (Medium-High Risk):* The NRA2 identified that t*he real estate market in Trinidad and Tobago is characterised by diverse property transactions for residential, commercial and industrial properties.* Real Estate Agents may deal with high-value transactions and complex ownership structures. Risks include the use of shell companies or trusts to obscure beneficial ownership. Mitigation measures include verifying the identity of all parties, conducting EDD on foreign buyers, and monitoring for unusual payment methods (e.g., large cash deposits).

6.2 Accountants *(Medium Risk): The NRA2 identified that Accountants may be involved in managing client funds or creating, operating and managing corporate structures,* which can be exploited to facilitate ML/TF/PF activities. Risks include facilitating the movement of illicit funds or creating opaque corporate structures. Controls should include verifying the source of funds, maintaining detailed records, and reporting suspicious activity.

6.3 *Jewellers (Medium Risk):* These businesses handle portable, high-value assets that are attractive to money launderers. Risks include cash purchases and lack of customer identification. Mitigation includes limiting cash transactions, verifying the origin of goods, and conducting CDD on buyers and sellers.

6.4 *Attorneys-at-Law (Medium Risk): The Second NRA identified that Attorneys-at-Law play a crucial role in facilitating legitimate business transactions and provision of services such as real estate transactions, trust and company formation and handling client funds,* which places the sector in a unique position of vulnerability to ML/TF/PF abuse. Risks include facilitating the creation of shell entities or nominee arrangements. Controls should include client screening, documentation of beneficial ownership, and monitoring for red flags.

NRFIs

6.5 *Credit Unions (Medium Risk):* Credit unions often operate in close-knit communities, which may lead to complacency in risk management. Risks include insider abuse[1] and lack of transaction monitoring. Controls should include PEP screening, transaction pattern analysis, and independent audits. *The NRA2 has identified some opportunities for improvement including standardizing background checks of members, enhancing training programmes and fostering sector-wide collaboration to address emerging risks more proactively.*

6.6 *Money Remittance (Medium Risk):* Some of the characteristics which expose these entities to ML/TF/PF risks include the predominant use of cash, cross-border nature, and reliance on agents and third-party networks. Mitigation measures include robust CDD procedures, including verification of sender and beneficiary identities, transaction monitoring for suspicious patterns, and screening against sanctions lists. H*owever, the NRA2 identified, that the total value of transactions and the average size of send and receive transactions are low, which does not make the remittance sector in Trinidad and Tobago an attractive vehicle for ML purposes. Notwithstanding, there is room for improvements in the quality of AML controls such as improvements in the AML knowledge of institution staff, the effectiveness of the compliance function and the effectiveness of suspicious activity monitoring and reporting.*

Dated 4 November, 2025
Financial Intelligence Unit of Trinidad and Tobago

[1] Insider abuse in a credit union refers to fraudulent, unethical, or unauthorized actions taken by individuals within the organization—such as employees, officers, directors, or other insiders—that exploit their access to systems, accounts, or decision-making authority for personal gain or to benefit others improperly.

APPENDIX I- SAMPLE RISK MATRIX AND RISK SCORING MODEL

A risk score can be derived from the risk matrix and risk scoring model shown below. Four levels of risk are shown, but the Supervised Entity should include as many as it believes may be necessary to support its business model.

Risk Matrix Template

RISK MATRIX		IMPACT		
		Low	Medium	High
LIKELIHOOD	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Extreme

Risk score/level and Response table

Risk Score	Risk Level	Response
4	Extreme The risk is almost certain to materialize and would result in severe consequences (e.g., significant legal, financial, or reputational damage).	**Immediate action required.** The business activity must be suspended or terminated unless the risk is mitigated to an acceptable level through robust controls. Escalate to senior management and consider reporting to relevant authorities.
3	High The risk is likely to occur and/or could lead to serious consequences.	**Restrict activity.** Do not proceed with the transaction (e.g. fund transfer, or service provision) until effective risk mitigation measures are implemented. EDD and senior-level review are recommended.
2	Medium The risk may occur and/or could result in moderate consequences.	**Proceed with caution.** The activity may continue, but risk mitigation steps must be taken. Apply standard due diligence and monitor for changes in risk profile.
1	Low	**Acceptable to proceed.** Routine controls and standard due diligence are sufficient. Continue monitoring as part of ongoing compliance.

	The risk is unlikely to occur and/or would have minor or negligible consequences.	