GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT OF TRINIDAD AND TOBAGO

Ministry of Finance

GUIDANCE ON A RISK BASED APPROACH TO COUNTER-PROLIFERATION FINANCING for REPORTING ENTITIES

Purpose

This Guidance is intended to provide assistance to Financial Institutions and Listed Businesses (collectively "Reporting Entities") on the implementation of measures to identify and mitigate against Proliferation Financing Risks.

Published 4 November, 2025
FIUTT REFERENCE: GN/004/2025

Table of Contents

1. INTRODUCTION AND PURPOSE

In an increasingly interconnected global financial system, the threat of proliferation financing ("PF")—the provision of funds or financial services used to support the proliferation of weapons of mass destruction—poses a significant risk to international peace and security. Recognising this, the Financial Action Task Force ("FATF") has strengthened its standards to ensure that countries and private sector entities take proactive steps to identify, assess, and mitigate PF risks.

In alignment with the FATF 40 Recommendations, Trinidad and Tobago enacted the Counter-Proliferation Financing Act, 2025 (Act No. 8 of 2025 hereinafter referred to as the "CPFA"). The CPFA was assented to on 22 October, 2025. The CPFA forms part of Trinidad and Tobago's Anti-Money Laundering, Counter Terrorist Financing and Counter Proliferation Financing ("AML/CFT/CPF") regime.

The Financial Intelligence Unit of Trinidad and Tobago ("FIUTT") is issuing this Guidance Note to financial institutions and listed businesses (Reporting Entities) to assist with the implementation of obligations set out in the CPFA, as well as in alignment with FATF Recommendation 1, which emphasize the application of a risk-based approach ("RBA") to PF. It also addresses the requirements of Recommendation 7, which mandates the implementation of targeted financial sanctions ("TFS")[1] without delay, in accordance with United Nations Security Council Resolutions.

The guidance herein is intended to support Reporting Entities in:

- Understanding the nature and scope of PF risks;
- Integrating PF risk assessments into their broader compliance programmes;
- Implementing proportionate and effective mitigation measures; and
- Ensuring timely and accurate compliance with TFS obligations.

By adopting these measures, Reporting Entities not only enhance their regulatory compliance but also contribute to the integrity and security of the national and international financial systems.

Reporting Entities are reminded that the implementation of a RBA is expected. The indiscriminate termination or restriction of business relationships with a class of customers, without assessing their level of risk and implementing proportionate risk mitigation measures is strongly discouraged.

In accordance with section 9 of the CPFA, "a financial institution or listed business shall develop and implement policies and programmes which are reasonably designed on a risk sensitive basis to manage and mitigate proliferation financing risks[2] to ensure compliance with this Act and any other written laws

[1] In accordance with section 2 of the Counter-Proliferation Financing Act, 2025, "targeted financial sanctions" means both asset freezing and prohibitions to prevent property or other assets from being made available, directly or indirectly for the benefit of listed entities and persons and entities acting on behalf of, or at the direction of listed entities in relation to proliferation financing, imposed under the Economic Sanctions Act or any other written law.

[2] In accordance with section 2 of the Counter-Proliferation Financing Act, 2025, "proliferation financing risk" means the potential breach, non-implementation or evasion of targeted financial sanctions in relation to proliferation financing, imposed under the Economic Sanctions Act or any other written law.

by which the recommendations of the Financial Action Task Force in relation to measures to counter proliferation financing are implemented."

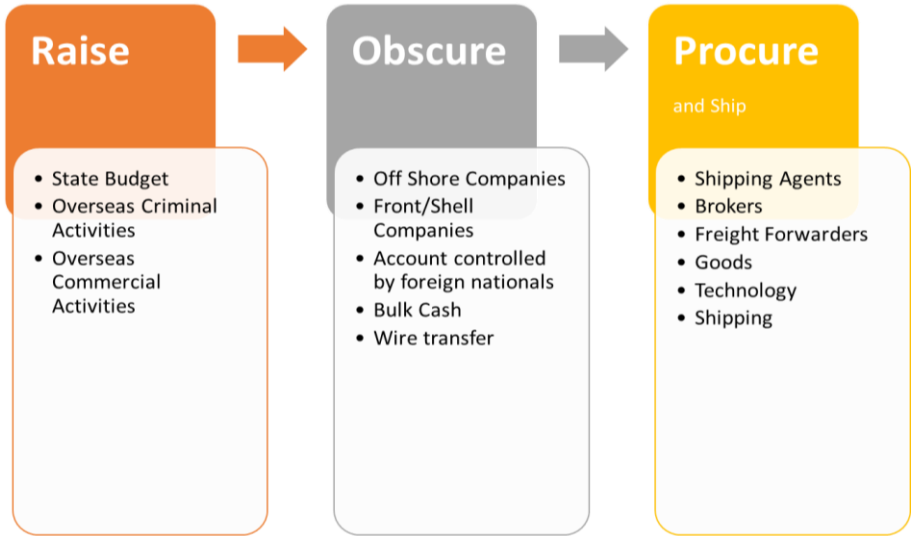
In order to implement such policies and programmes, Reporting Entities are required to implement measures commensurate with the Money Laundering ("ML") and Terrorist Financing ("TF") obligations set out in the Financial Obligations Regulations 2010 ("FORs") for the purposes of mitigating proliferation financing risks. This means that the obligations, prohibitions and offences in the FORs should be read as not only including ML and TF but also PF and TFS as it related to PF.

The Compliance Officer has the responsibility of ensuring the necessary compliance programme procedures and controls required by the FORs are in place. Therefore, the Compliance Officer should also adhere to the contents of this document when assessing the ML/TF/PF risks of the Reporting Entity, with a view to incorporating an assessment of PF risks into the ML/TF Entity Risk Assessment. The Compliance Officer should also ensure that the applicable procedures and controls for CPF risks identified are included in the AML/CFT/CPF Compliance Programme. The goal should be the development of a comprehensive AML/CFT/CPF Compliance Programme.

2. UNDERSTANDING THE NATURE AND SCOPE OF PF RISKS

STAGES OF PROLIFERATION FINANCING

Proliferation Financing involves three (3) stages:



First stage: the proliferator raises funds for the proliferation programme through its own budget, its overseas corporate network or its overseas criminal activity.

Second stage: funds are transferred in the international financial system. This is the stage that presents the highest risk for gatekeepers, i.e., Financial Institutions, TCSPs, Accountants, etc.

Common, known methods used by proliferators at this stage include the use of front and shell companies, intermediaries, opaque ownership structures, transactions with geographic locations bordering or near a sanctioned country, false documentation, etc.

Third stage: the proliferator uses the funds to pay for goods, materials, technology, and logistics needed for the weapons of mass destruction ("WMD") programme. A very important characteristic of this stage is that it involves not only the purchase of weapons, but also of individual goods, technology and component parts that can be used in the development of weapons or missiles.

PROLIFERATION FINANCING RISKS

PF risks differ from ML and TF risks. PF risk arises when Reporting Entities, or other entities **unwittingly or deliberately facilitate the financing of the proliferation of WMDs, leading to:**

- **Breach or non-implementation of TFS** imposed by the United Nations Security Council and Trinidad and Tobago pursuant to an Order made under section 4 of the Economic Sanctions Act;
- **Evasion of sanctions** through deceptive practices, such as the use of front companies, complex trade structures, or falsified documentation.

Proliferation financing may involve:

- **State actors or sanctioned entities**;
- **Use of front companies or intermediaries**;
- **Dual-use technologies and goods** (civilian and military applications) for non-legitimate purposes; or
- **Complex trade and shipping routes**.

2.1 Potential Vulnerabilities of Reporting Entities to PF Risks

A clear understanding of entity specific PF risks, coupled with the effective implementation of proportionate mitigation measures, is essential to avert the following three key adverse consequences: a breach of TFS, the non-implementation of TFS and the evasion of TFS.

1. Breach of TFS

A breach occurs when a Reporting Entity **fails to freeze assets or allows transactions** involving designated persons or entities. This may happen due to:

- Inadequate screening systems or failure to report or freeze the assets of designated persons 'without delay'[3];
- Reference to outdated sanctions lists; and
- Lack of awareness or training.

2. Non-Implementation of TFS

[3] The phrase 'without delay means', ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee and should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to the financing of proliferation of weapons of mass destruction. Source: Summarized from FATF Glossary

Non-implementation refers to **systemic or procedural failures** to apply TFS obligations. This includes:

- Not integrating TFS into internal controls;
- Failing to conduct due diligence on customers and transactions;
- Ignoring updates to sanctions regimes.

3. Evasion of TFS

Sanctions evasion involves **deliberate attempts by designated entities to circumvent controls**, often through:

- Use of intermediaries or shell companies;
- Misuse of trade finance instruments;
- Concealment of beneficial ownership;
- Manipulation of shipping routes and documentation.

In order to manage these adverse consequences most effectively, Reporting Entities are encouraged to implement the measures outlined in this Guidance Note.

2.2 Establish a PF Risk Assessment Framework

Reporting Entities should develop a structured framework to assess their specific PF Risks[4] in accordance with regulation 7(2) of the FORs. This framework should be tailored to the specific characteristics of their operations, including their sector, products and services, cross-border activities, and customer base. ***The framework should also consider the results of the National Risk Assessment and any other PF risk assessments conducted by the FIUTT or another Competent Authority.***

The Risk Assessment Framework should include:

Risk Identification

- **<u>Sector-specific risk profiling:</u>**

  Each sector has unique exposure to PF risks. Some sectors may have low or no exposure to risks, while others may have greater risk exposure. For example, **Banks** may face risks through trade finance, wire transfers, and correspondent banking. **Real estate agents** may be exposed through high-value transactions involving opaque ownership. **Trust and Company Service Providers** may be exposed to PF risks through the provision of services to companies which may be beneficially owned or controlled by designated persons. **Dealers in precious metals and stones** may be vulnerable to PF through high-value, portable assets, which provide an alternative method for moving financial assets across international borders.

  Reporting Entities should map their sector specific vulnerabilities using PF typologies[5], FIUTT publications as well as the results of the National Risk Assessment or any other PF Risk Assessment published by a Competent Authority.

[4] Based on the FATF Standards, Reporting Entities are directed to a narrow definition of PF risk, strictly requiring the understanding of the Reporting Entity's risk of breach, non-implementation or evasion of Targeted Financial Sanctions related to PF.

[5] For example: Study of Typologies of Financing of WMD Proliferation, King's College London, 13 October 2017

- **Customer Risk:**
  Exposure to customers who operate in high-risk sectors (e.g., defence, chemicals, dual-use goods), or customers with opaque ownership structures such as companies or trusts with multi-layered ownership, or customers with links to sanctioned jurisdictions, pose a higher risk to the Reporting Entity for being used as a conduit for proliferation financing and sanctions evasion.

  Reporting Entities customer risk scoring models should incorporate PF specific risk indicators, such as links to high-risk sectors or jurisdictions to risk-rank their customers.

- **Product/Service Risk:**
  Use of services that can obscure the origin or destination of funds (e.g., Trade finance, international wire transfers, letters of credit, and complex investment vehicles). Each product and service offered by the Reporting Entity may be subject to a different level of PF risk.

  Reporting Entities should assign risk ratings to their specific products and services based on their potential misuse for PF. Each product or service offered should be assessed based on their inherent risk factors, such as, anonymity, portability of value, complexity, cross border use and association with high risk sectors.

- **Geographic Risk:**
  Operations in, or transactions with countries subject to UN sanctions or known for weak export controls.

  Reporting Entities should create a geographic risk matrix of the countries from and with which they conduct business which categorises them as:
  - *High Risk: Sanctioned jurisdictions, weak controls, known PF activity;*
  - *Medium Risk: Countries with limited controls or indirect exposure; and*
  - *Low Risk: Countries with strong regulatory frameworks and active enforcement.*

- **Delivery Channel Risk**:
  The use of non-face to face transactions, intermediaries or agents, complex transaction chains, high speed or automated channels and informal value transfer systems may pose specific risks for PF. Sanctioned entities may exploit digital platforms to access financial services anonymously or through false identities. Intermediaries can be used to mask the true originator or beneficiary of a transaction, facilitating sanctions evasion. Funds may be routed through several delivery channels to avoid detection or exploit regulatory gaps. Rapid movement of funds can outpace detection systems, especially if sanctions lists are not updated in real time. Informal Value Transfer systems such as *hawala* can be used to move funds covertly, especially in regions with limited financial infrastructure.

Reporting Entities should identify all delivery channels used for their products and services and assign risk ratings based on the potential for anonymity, geographic exposure, control over intermediaries used, the Reporting Entity's ability to conduct real time sanctions screening, and the volume and speed of the transaction involved.

Risk Analysis and Evaluation

After identifying its risks, a Reporting Entity should conduct an analysis of its risks using its internal data, e.g. an observation of its transaction patterns to determine how often it is exposed to the risks identified; a review of its customer risk profiles to determine what percentage of its customer base may be high, medium or low risk for PF; and also review external source materials to determine whether it may be exposed to any trends, typologies or advisories on PF risks in its sector which it may not have previously considered (e.g. FIUTT advisories, FATF typologies, updated to PF Sanctions Lists). The Reporting Entity should then assign risk ratings to its customer types, products, and services (e.g. High, Medium Low) based on its understanding of its PF exposure.

Documentation, Review and Update

PF risks should be integrated into the Reporting Entity's overall AML/CFT risk assessment. Treat PF as a distinct, but related risk, alongside money laundering and terrorist financing risks. Include PF specific risk factors, but use the same risk rating methodology (e.g. low, medium, high) to ensure consistency.

Ensure the risks which have been identified are broken down by category, assign risk scores to each category and justify ratings with data or examples. The Risk analysis should identify the high risk areas the Reporting Entity is exposed to and require the implementation of enhanced controls (the methods of Enhanced Due Diligence (EDD) to be used) for these areas.

The PF risk assessment and subsequent updates should be documented, reviewed and approved by senior management[6].

All PF risk assessment information, including the documented PF Risk Assessment, should be kept in a manner which permits the Reporting Entity to easily provide to the FIUTT or other Competent Authorities, when requested.

[Intentionally left blank]

[6] According to section 55C(3) of the Proceeds of Crime Act, Chap.11:27, "senior management" refers to the body responsible for directing or overseeing the performance of the Reporting Entity.

3. INTEGRATING PF RISK ASSESSMENTS INTO THE BROADER COMPLIANCE PROGRAMME

After understanding its PF risks, the Reporting Entity should incorporate PF risk considerations into its AML/CFT compliance programme. Risks identified should be subject to appropriate mitigation procedures, e.g. EDD for high risk areas, greater on-boarding protocols for high-risk clients or products and PF specific transaction monitoring rules to detect PF red flag.

A breach of sanctions or non-implementation often happens because of weak internal systems. This can include inadequate CDD, delays in screening, reporting and freezing assets of designated entities, using outdated sanctions lists to screen against, or errors in matching names.

To reduce these risks, Reporting Entities should establish risk based controls, and independent periodic reviews in accordance with regulation 10 of the FORs, to ensure compliance.

In keeping with regulation 7(1) of the FORs with a view to incorporating PF risk mitigation measures, the Compliance Programme should include policies, procedures and controls for the following as it relates to the PF risks identified:

1. Customer identification, documentation and verification of customer information and other customer due diligence (CDD) measures designed to identify information, including information on the customer's counterparty and high risk jurisdictions where the customer is doing business, which would enable the Reporting Entity to identify where the customer's risk for attempting to evade sanctions or commit breaches of PF sanctions may be higher.

   This includes ensuring sufficient measures are taken to identify the Beneficial Owner(s) of the customer in accordance with regulation 12 of the FORs.

   Adequate and timely screening of customers against the PF sanctions list is also a necessary part of the CDD process. The Anti-Terrorism Unit, Office of the Attorney General, Ministry of Legal Affairs maintains a list of all individuals and entities listed pursuant to these Orders. See link here: https://agla.gov.tt/anti-terrorism-unit/atu-proliferation-financing-of-weapons-of-mass-destruction/atu-proliferation-financing-of-weapons-of-mass-destruction/

   The enhanced actions which are required to be taken for a customer identified as high risk should be clearly documented.

2. Identification and internal reporting of suspicious transactions and suspicious activities ("STR/SAR") which may indicate sanction evasion or breaches and attempts to commit sanction evasion and breaches. There should be clear channels and procedures for making such internal reports to the Compliance Officer, who should consider the reports and determine whether an STR/SAR should be filed with the FIUTT.

3. Adoption of a risk-based approach to monitoring financial activities that are considered a high risk for PF sanctions evasion, non-implementation and breaches. Enhanced monitoring should be applied for the higher risk customers, products, services and delivery channels identified in the PF

risk assessment. These measures should be clearly documented in the Compliance Programme to ensure they are effectively implemented by relevant staff.

4. Independent testing of the measures implemented on a periodic basis to ensure that measures taken (e.g. on-boarding procedures and transaction monitoring) are in line with the CPF measures stated in the Compliance Programme. Independent testing ensures that the relevant staff and other resources are adequately and effectively implementing the CPF procedures in accordance with the PF risks identified.

5. An effective risk-based audit function to evaluate the CPF measures recommended in the Compliance Programme. While independent testing of the measures implemented can ensure the compliance programme is being adhered to, an audit of the compliance programme itself can ensure that the policies within the compliance programme continue to be adequate and effective to mitigate against the identified risks of PF sanctions evasion, breaches and non-implementation. This audit can recommend updates and changes to the CPF policies where necessary.

6. Internal controls and communication as may be appropriate for the purposes of forestalling PF, including attempts to breach or evade PF sanctions.

7. The retention of transaction records and other information. The record keeping measures contained in the Compliance Programme for CPF should be in accordance with the FORs, including regulations 31 and 32.

8. Measures to be applied in respect of any jurisdictions identified by a Competent Authority or the United Nations Security Council as being high risk for PF.

9. The adoption of risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification – bearing in mind that ***transactions should not be permitted if PF sanctions breach or evasion is suspected.***

10. Ongoing training for staff on PF risk identification and the mitigation measures set out in the Compliance Programme. This training should be tailored to the various levels of staff across business lines so that there is an appropriate and effective level of understanding of the measures to be applied. The training should be updated with any changes made to the Compliance Programme and should be conducted periodically to ensure staff knowledge remains relevant and consistent.

N.B. there is no need to create a separate Compliance Programme specific to CPF. The measures above should be documented and implemented alongside the Reporting Entity's existing AML/CFT Compliance Programme, effectively creating a comprehensive AML/CFT/CPF Compliance Programme.

4. IMPLEMENTING PROPORTIONATE AND EFFECTIVE MITIGATION MEASURES

Risk mitigation measures should be applied proportionate to the PF risks identified. The Compliance Programme (as discussed above) should contain enhanced procedures for high risk customers, products and services as well as effective transaction monitoring for those high risk areas identified.

However, Reporting Entities who have established low risk for PF sanctions evasion, breaches and non-implementation and serve predominantly lower risk customers do not need to devote significant resources to risk mitigation and may choose to rely on their sanctions screening measures and other CDD measures without implementing additional measures.

Reporting Entities are reminded that simplified due diligence measures should never be applied where there is a suspicion of ML/TF/PF.

5. ENSURING TIMELY AND ACCURATE COMPLIANCE WITH TFS OBLIGATIONS

Notwithstanding the risk based measures recommended above, Reporting Entities **must** comply with the TFS obligations set out in **the Economic Sanctions (Implementation of United Nations Resolutions on the Democratic People's Republic of Korea) Order, 2018** and **the Economic Sanctions (Implementation of United Nations Resolutions on the Islamic Republic of Iran) Order, 2023**.

These Orders direct all Reporting Entities to implement measures to prevent and disrupt PF through the application of TFS against the individuals and entities listed in Trinidad and Tobago pursuant to these Orders. Reporting Entities are required to undertake due diligence to confirm whether it is in possession of property –

(a) wholly or jointly owned or controlled, directly or indirectly, by a person who appears on the PF Lists maintained and circulated by the Office of the Attorney General ("listed entity");
(b) derived or generated from funds owned or controlled directly or indirectly by listed entities; or
(c) of persons or entities acting on behalf of, or at the direction of listed entities.

Reporting Entities are required to screen all customers against the aforesaid lists as part of its CDD procedures at on-boarding or when undertaking a transaction which does not have a low PF risk.

The FIUTT circulates notifications to all Reporting Entities when an update is made to this list. All Reporting Entities are required to screen ***all customers*** against the updates to the list **immediately** upon receipt of the updates.

These screening measures are required to enable the Reporting Entity to detect whether it is holding property belonging to, or conducting a transaction on behalf of, a listed entity, or any person or entity acting on behalf of or at the direction of a listed entity.

Upon screening against this list, if a Reporting Entity discovers that it is holding property belonging to, or conducting a transaction on behalf of, a listed entity, or any person or entity acting on behalf of or at the direction of a listed entity, it must ***immediately freeze*** such property, ***cease the transaction*** and ***file an Economic Sanctions Report*** with the FIUTT.

If a Reporting Entity has a ***suspicion*** that it is holding property belonging to, or conducting a transaction on behalf of, a listed entity, or any person or entity acting on behalf of or at the direction of a listed entity, it must ***immediately file a STR/SAR*** with the FIUTT.

For guidance on compliance with these Orders please consult the FIUTT's Guidance to Financial institutions and Listed Business on Sanctioned Entities Pursuant to Orders Made Under the Economic Sanctions Act, Chap. 81:05.

6. OFFENCES AND PENALTIES

Section 12 of the CPFA sets out both criminal and administrative penalties for failure to comply with the provisions of section 5 (Reporting STR/SARs to the FIUTT) and section 9 (development, implementation and approval of risk based policies and programmes to mitigate PF Risks)

The criminal penalty for knowingly contravening or failing to comply with sections 5 and 9 of the CPFA is-

(a) on summary conviction, to a fine not exceeding two million dollars and to imprisonment for a term not exceeding two years; or
(b) on conviction on indictment, to a fine not exceeding five million dollars and to imprisonment for a term not exceeding seven years.

REFERENCES

FATF (2025), Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems, FATF, Paris, www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-Methodology-2022.html

FATF (2021), Guidance on Proliferation Financing Risk Assessment and Mitigation, FATF, Paris, France, https://www.fatf-gafi.org/publications/financingofproliferation/documents/proliferation-financing-riskassessment-mitigation.html

Financial Obligations Regulations, 2010, made under section 56 of the Proceeds of Crime Act, Chap. 11:27, Laws of the Republic of Trinidad and Tobago https://laws.gov.tt/ttdll-web/revision/download/117070?type=amendment

The Counter-Proliferation Financing Act, 2025, Act No. 8 of 2025 Laws of Trinidad and Tobago

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