COUNTERING PROLIFERATION FINANCING GUIDELINES

FOR FINANCIAL INSTITUTIONS AND DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

Prepared by:
Group of Financial Services Regulators
Year of Publication: 2025

CENTRAL BANK OF THE BAHAMAS
SECURITIES COMMISSION OF THE BAHAMAS
INSURANCE COMMISSION OF THE BAHAMAS
COMPLIANCE COMMISSION OF THE BAHAMAS
GAMING BOARD FOR THE BAHAMAS

About the Group of Financial Services Regulators (GFSR)

This Guidance is issued by the Group of Financial Services Regulators (GFSR). The members of the GFSR are the Central Bank of The Bahamas, Securities Commission of The Bahamas, Insurance Commission of The Bahamas, Compliance Commission of The Bahamas, and Gaming Board for The Bahamas. The Financial Intelligence Unit (FIU) is a permanent observer to the GFSR. The FIU attends all meetings and participates in GFSR activities, as appropriate.

The GFSR aims to promote financial stability and improve the efficiency and effectiveness of financial regulation in The Bahamas through information sharing agreements, and processes to collaborate and cooperate. The Group is uniquely positioned to identify, monitor and address systemic risk in the financial services sector. The GFSR also works to harmonize regulatory practices, to minimize supervisory overlap and foster greater efficiency in financial services regulation and supervision.

Each GFSR member is empowered, through legislation, to supervise and regulate its licensees and registrants in line with relevant laws and policy guidelines, including The Bahamas' frameworks for anti-money laundering, countering the financing of terrorism, and countering proliferation financing (AML/CFT/CPF).

The members of the GFSR are signatories to a Memorandum of Understanding (MoU), which establishes the framework by which information may be shared between the regulators to effectively supervise the financial services sector in The Bahamas. The MoU also outlines the arrangement for consolidated supervision of systemically important financial services institutions and conglomerates in The Bahamas, including, but not limited to, regular communication, monitoring capital and inter-group transactions and, where appropriate, mutual decision-making regarding supervisory approvals and reprimands.

Table of Contents

Glossary – Key Abbreviations

Objective: This section provides key abbreviations consistently used throughout this publication.

TERM	DEFINITION/INTERPRETATION
AML/CFT/CPF	Anti-Money Laundering/Countering the Financing of Terrorism/Countering Proliferation Financing
ATA	Anti-Terrorism Act 2018
CBA	Central Bank of The Bahamas Act 2020
CC	Compliance Commission of The Bahamas
Central Bank	Central Bank of The Bahamas
CDD	Customer Due Diligence
CFATF	Caribbean Financial Action Task Force
CO	Compliance Officer
DARE Act	Digital Assets and Registered Exchanges Act 2024
DARE Rules	Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering Financing of Terrorism and Countering Financing of Proliferation) Rules 2022
DNFBPs	Designated Non-Financial Businesses and Professions
DPRK	Democratic People's Republic of Korea
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FCSPA	Financial and Corporate Service Providers Act 2020
FIU	Financial Intelligence Unit
FTRA	Financial Transactions Reporting Act 2018
GBB	Gaming Board for The Bahamas
GFSR	Group of Financial Services Regulators
ICB	Insurance Commission of The Bahamas
IFA	Investment Funds Act 2019
IRF STEERING COMMITTEE	Identified Risk Framework Steering Committee
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
ML/TF/PF	Money Laundering/Terrorist Financing/Proliferation Financing
NRA	National Risk Assessment
POCA	Proceeds of Crime Act 2018
SCB	Securities Commission of The Bahamas
SFI	Supervised Financial Institution
SIA	Securities Industry Act 2024
STR	Suspicious Transaction Report
TFS	Targeted Financial Sanctions
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
WMD	Weapons of Mass Destruction

Glossary – Key Terminology

Objective: **This section provides definitions of key terminology used throughout this guidance.**

TERM	DEFINITION/INTERPRETATION
COMPETENT AUTHORITIES	Refer to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing and/or proliferation financing, namely Central Bank of The Bahamas, Securities Commission of The Bahamas, Insurance Commission of The Bahamas, Compliance Commission of The Bahamas, Gaming Board for The Bahamas, Financial Intelligence Unit, and Office of the Attorney General.
DIGITAL ASSET BUSINESS	According to Section 6 of the DARE Act, a digital asset business includes the business of a digital token exchange, providing services related to a digital token exchange, operating as a payment service provider utilizing digital assets, operating as a digital asset service provider, or participation in and provision of financial services related to an issuer's offer or sale of a digital asset.
DESIGNATED ENTITIES	Individuals or entities and their associates designated as terrorist entities by the United Nations' Security Council (UNSC).
IDENTIFIED RISK	Has the same meaning as defined in both the Proceeds of Crime Act 2018 (POCA) and the Financial Transactions Reporting Act 2018 (FTRA) and includes: corruption, cybercrime, human trafficking, money laundering, financing of proliferation of weapons of mass destruction, terrorism, financing of terrorism or such other risk as prescribed.
FIU	The Financial Intelligence Unit is responsible for receiving, analyzing, obtaining and disseminating information, which relates to or may relate to the proceeds of the offences in the POCA and under the Anti-Terrorism Act (ATA).
NON-STATE ACTORS	Individuals or entities conducting activities falling within the scope of UNSCR 1540 without lawful authority from any state.
PROLIFERATION	The transfer and export of nuclear, chemical, or biological weapons, their means of delivery, and related materials.
PROLIFERATION FINANCING	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.
TARGETED FINANCIAL SANCTIONS	The act of asset freezing, blocking, and rejecting of transactions and persons to prevent, suppress, and disrupt the proliferation of weapons of mass destruction and its financing in line with sanctions, such as those imposed by the UNSC.

1 Background

The Group of Financial Services Regulators (GFSR) publishes these updated guidelines to provide guidance to facilitate both public and private sector stakeholders (together, stakeholders) in identifying, assessing, understanding and mitigating their proliferation financing risks. The guidelines also aim to facilitate stakeholders in implementing their proliferation financing obligations.

In 2018, the GFSR released a Guidance Note on Proliferation and Proliferation Financing (the 2018 Guidance Note), which was intended to raise awareness of the risks and vulnerabilities created by proliferation and proliferation financing, describe indicators of possible proliferation financing risks, and illustrate the potential damage to The Bahamas if a regulated entity plays an appreciable role in the activity. The 2018 Guidance Note also provided common definitions surrounding proliferation financing, described the regulatory framework in The Bahamas as it related to proliferation financing, and described international standards and best practices to identify, assess, understand and combat proliferation and proliferation financing. Since its publication in 2018, there have been updates to the Bahamian CPF regime and the Financial Action Task Force (FATF) has provided further guidance. These updated Guidelines seek to guide the financial services industry on the regime for countering proliferation financing (CPF), provide clarity on expectations and changes made, and bring The Bahamas into further compliance with the FATF.

In October 2020, the FATF revised Recommendation 1 (R.1.) and its Interpretive Note (INR.1) to, among other things, develop a common understanding about the impact of the amendments to R.1 and INR.1. In particular, how countries and private sector entities should implement the new requirements to assess and mitigate proliferation financing risks given the rule-based nature of the targeted financial sanctions (TFS) under Recommendation 7 (R.7). The FATF also made a minor consequential amendment to Recommendation 2 (R.2), to insert reference to counter proliferation financing in the context of national cooperation and coordination, and added a new interpretive note that sets out the inter-agency framework to promote cooperation, coordination and information exchange. The GFSR reviewed the updated Recommendations in tandem with The Bahamas' CPF framework, and made amendments to the various legislation, namely the Anti-Terrorism Act 2018 (ATA), the Financial Transactions Reporting Act 2018 (FTRA) and the Proceeds of Crime Act 2018 (POCA), which led to The Bahamas' rating to change from partially compliant with R.7 to largely compliant, and maintained the rating of compliant with R.2.

As new products and developing technologies emerge, standard setting bodies continue to update their guidance on best practices to identify and combat proliferation financing. The GFSR is committed to ongoing review and incorporation of these updates where applicable, and informing stakeholders of their new and continuing obligations. In light of this, the GFSR issues these guidelines to provide the requirements for relevant financial services providers to comply with the obligations imposed under the relevant financial services laws of The Bahamas, thereby managing PF risks and threats.

Inclusion of Digital Asset Businesses

The Digital Assets and Registered Exchanges Act 2020 (DARE Act) was adopted in November 2020. The DARE Act regulates the issuance, sale, and trade of digital assets in or from within The Bahamas. The DARE Act also prescribes a regulatory framework for persons and entities engaged in digital asset business. In order to maintain the country's robust anti-money laundering, countering financing of terrorism, and countering proliferation financing (AML/CFT/CPF) framework, a priority of 2021 was to capture the digital

asset regime in the AML/CFT/CPF framework through the Fifth Schedule, the Corrigendum to the DARE Act. This ensures that digital asset businesses and prescribed activities are included in the country's proliferation financing legislative framework at the national level.

Protecting the country's reputation in financial services remains a priority as we continue to develop our markets. To date, the GFSR can proudly state that the country has not identified major red flags in relation to proliferation financing; however, publishing updated guidelines ensures the regime remains current. The Bahamas has continued to progress in strengthening its framework for money laundering and terrorist and proliferation financing risks, as evident in the country's 2022 follow-up report published by the Caribbean Financial Action Task Force (CFATF) showing that The Bahamas is rated either compliant or largely compliant with all 40 of the FATF's Recommendations.

The GFSR intends to continue this trend of compliance; and it is anticipated that these Guidelines provide the necessary clarity for the industry, and country at large, to carry out its mandated obligations. The GFSR will continue to do its part in keeping the relevant legislation both updated and robust, in line with international best practices, thus establishing The Bahamas as the jurisdiction of choice for financial services.

2 Introduction

The FATF defines proliferation as "the transfer and export of nuclear, chemical, or biological weapons, their means of delivery and related materials."[1] Moreover, the United Nations Security Council (UNSC) affirmed that proliferation poses a significant threat to international peace and security.[2] UNSC resolutions serve as a call to all member states to take additional measures to prevent proliferation wherever possible. The proliferation financing activities of certain state actors[3] have highlighted the need for strategies to combat proliferation financing on a global scale.

Recommendation 7 of the FATF Recommendations requires jurisdictions to implement TFS related to proliferation financing made under UNSCRs. Recommendation 2 requires jurisdictions to adopt national cooperation and coordination mechanisms to combat financing the proliferation of WMDs. Immediate Outcomes 1 and 11 measure the effectiveness of countries in implementing the Recommendations.[4]

In June 2018, the FATF issued non-binding guidance (2018 FATF Guidance) to facilitate both public and private sector stakeholders in understanding and implementing their CPF obligations. In response, in August 2018, the GFSR issued a guidance note to existing and prospective registrants and licensees. This note, among other things, "provided common definitions surrounding proliferation financing and described the regulatory framework in The Bahamas, coupled with international standards and obligations that are relevant to combatting proliferation financing risks."[5] Notably, the 2018 FATF

[1] This includes, inter alia, technology, goods, software, services, or expertise. See 2008 FATF Proliferation Financing Report CHttpHandler.ashx (gov.gg).
[2] See Security Council Resolution 1540 - UNSCR.
[3] In particular, Iran, The Democratic People's Republic of Korea, and Russia.
[4] FATF (2018), Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, FATF, Paris.
[5] Guidance Note on Proliferation and Proliferation Financing, August 21, 2018.

Guidance neither required countries to assess their proliferation financing risks nor to apply risk-based[6] TFS.

In October 2020, the FATF updated its Standards (2020 Standards) to require that both countries and private sector entities identify, assess and understand the proliferation financing risks they face. They are also required to take action to mitigate the identified risks. The 2020 Standards do not prescribe a specific risk methodology, but instead recommend that individual countries develop a customized methodology that considers the nature, scope and size of the activity identified.

Regularly identifying, assessing and understanding proliferation financing risks is essential to strengthening a country's ability to prevent designated persons involved in proliferation from accessing, storing, transferring and utilizing funds and other assets. Implementing TFS related to proliferation and its financing is crucial for a robust CPF regime.

While The Bahamas has yet to experience direct negative consequences of proliferation, the threat of proliferation financing remains non-zero. As a major global financial hub, The Bahamas has a responsibility to address the potential for PF within the jurisdiction. Financial regulators, financial institutions, and individuals within the jurisdiction also have a responsibility to identify and monitor PF vulnerabilities and implement safeguards against The Bahamas' involvement in such activity. As new complex financial products emerge, jurisdictions must remain vigilant when applying their counter proliferation principles.

2.1 Purpose, Objectives, and Scope

These Guidelines serve several purposes, including:

- Defining proliferation and proliferation financing;
- Explaining PF risks and key indicators;
- Describing the role of the financial services regulators in the jurisdiction in combating PF;
- Describing the key concepts relevant to assessing PF risks;
- Highlighting the regulatory framework that supports CPF; and
- Offering sector guidance for members of relevant subsections of the financial services industry in The Bahamas, namely all sectors regulated by the Central Bank of The Bahamas, Securities Commission of The Bahamas, Insurance Commission of The Bahamas, Compliance Commission of The Bahamas, and Gaming Board for The Bahamas.

2.2 Role of the Group of Financial Services Regulators

Formed in 2001, the GFSR[7] comprises the financial market regulators in The Bahamas. Its primary objectives are to promote financial sector stability through timely and effective exchange of information among regulators, coordinate supervisory efforts, and devise responses to potential systemic risks. Each member is tasked with supervising and regulating their respective licensees and registrants in accordance with relevant laws, policies and guidelines.

[6] The requirement was rule-based.

[7] GFSR comprises the Central Bank of The Bahamas, Securities Commission of The Bahamas, Insurance Commission of The Bahamas, Compliance Commission of The Bahamas, and the Gaming Board for The Bahamas. The Financial Intelligence Unit has been granted an observer status at GFSR meetings.

Along with their individual responsibilities, GFSR members are bound by a signed Memorandum of Understanding (MoU), which requires them to, inter alia:

- Foster regular communication and cooperation amongst members;
- Monitor capital and inter-group transactions; and
- Engage in mutual decision-making regarding supervisory approvals and reprimands, where applicable.

In matters of national importance, members collaborate and cooperate to, inter alia, release comprehensive sector-specific guidance for The Bahamas' financial services industry in areas of anti-money laundering, countering the financing of terrorism and countering proliferation financing (AML/CFT/CPF).

2.3 Role of Identified Risk Framework Steering Committee

The Identified Risk Framework Steering Committee (IRF Steering Committee), established and mandated by the Proceeds of Crime Act 2018, is a collaborative team comprised of representatives from various regulatory and enforcement authorities in The Bahamas. The IRF Steering Committee is tasked with several responsibilities:

- Periodically coordinating a national risk assessment (NRA) to identify, assess and understand the identified risks, ensuring that such assessments remain updated and relevant;
- Maintaining surveillance of FATF pronouncements regarding the application of enhanced due diligence to the country's risks;
- Receiving and collating reports from industry stakeholders of persistent regulatory failures by a jurisdiction or foreign financial institution, and compiling a list of such jurisdictions or foreign financial institutions;
- Advising financial institutions of their obligations to apply enhanced due diligence to transactions originating from jurisdictions or foreign financial institutions named by the IRF Steering Committee and the FATF;
- Coordinating the development, regular review and implementation of national policies and activities to mitigate identified risks;
- Collecting and analysing statistics and other information from competent authorities to assess the effectiveness of the identified risk framework;
- Coordinating measures to identify, assess and understand the impact of prescribed provisions of the POCA; and
- Establishing appropriate mechanisms for providing information on identified risks to relevant financial institutions, self-regulatory bodies and professional associations.

The IRF Steering Committee is tasked with identifying, assessing and implementing appropriate mitigating measures to address the financial sector risks to which the jurisdiction is exposed.

3 Overview of Proliferation Financing

Preventing proliferation financing is essential to maintaining global security and preventing the distribution of weapons of mass destruction (WMDs). As a key trade and finance hub in the region, The

Bahamas must remain vigilant in identifying and preventing the transfer of funds or materials, while ensuring the security and stability of its financial systems.

3.1 Proliferation

As previously defined, proliferation relates to the transfer of, or facilitating the transfer of, technology, goods, software, services, or expertise that can be used in programs developing WMDs. Proliferation supports the actions of bad actors on an international scale. Inhibiting the activities that support proliferation, including proliferation financing, aligns with the goals of the GFSR, the IRF Steering Committee and international bodies such as the FATF.

3.2 Proliferation Financing

The 2010 FATF Status Report on Combating Proliferation Financing[8] provides a working definition of proliferation financing. It is:

"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".

Proliferation financing provides bad actors with the opportunity to acquire nuclear, chemical, or biological weaponry, or to acquire the knowledge necessary to produce them. Proliferation financing, therefore, represents a significant threat to global stability and peace, as there is evidence to suggest that terrorists

[8] See Combating Proliferation Financing: A Status Report on Policy Development and Consultation (fatf-gafi.org).

and terrorist organizations have sought to use WMDs in acts of terrorism.[9] Financial authorities, therefore, play a pivotal role maintaining global stability.

Financial authorities can inhibit the movement of funds related to ML, TF, and PF through adopting international standards and collaborating with international regulatory bodies. In doing so, financial institutions and DNFBPs will also be obligated to incorporate a risk-based approach when dealing with customers and potential customers. Through vigilantly monitoring customer and potential customer activities using a risk-based approach, financial institutions, DNFBPs, and authorities can inhibit the flow of funds intended for illicit purposes.

3.2.1 Dual Use Goods

Implementing appropriate safeguards concerning dual use goods is crucial in the fight against proliferation and proliferation financing within a jurisdiction. Dual use goods are products, technology, or equipment that can serve both civilian and military applications. Examples include items such as lasers, electronics, radio navigation systems, and common household materials that can be easily repurposed to make weapons. Proliferators often exploit these goods in circumvention of TFS. Consequently, trade in these goods must be heavily monitored by relevant government agencies.

While it can be difficult to determine a customer's intended usage of dual use goods when purchased, there may be instances where financial institutions and DNFBPs can flag certain transactions (e.g. wire transfers) for review. To keep abreast of these goods, financial institutions and DNFBPs may review The Bahamas Customs' list of prohibited and restricted imports and exports.[10]

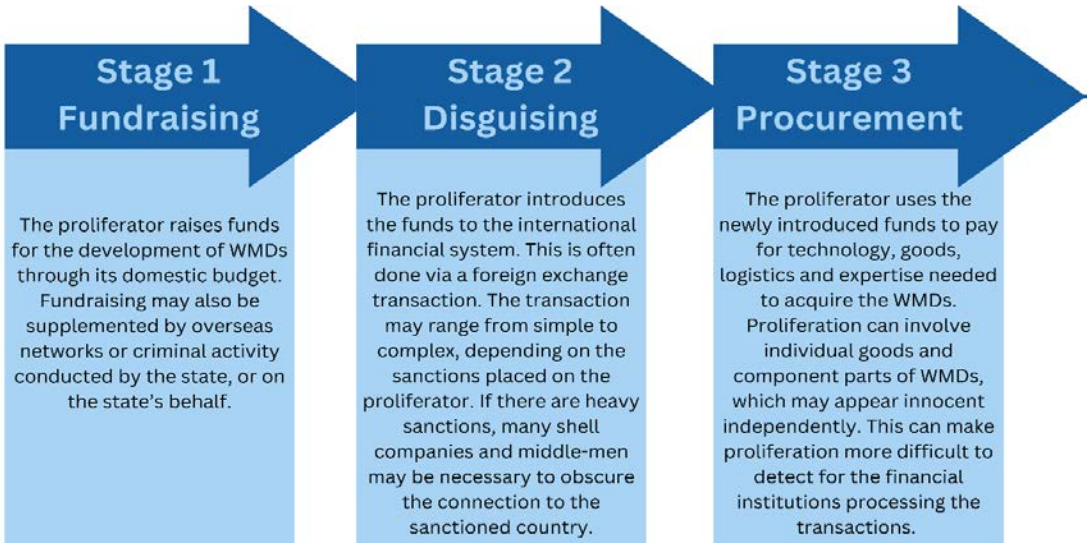
3.3 Stages of Proliferation Financing

There are three stages of proliferation financing: fundraising, disguising, and procurement.[11] The following illustration summarizes these three stages:

[9] Examples include Abdul Qadeer Khan, and WMD procurement by Iran and the Democratic People's Republic of Korea via proliferation financing. See AQ Khan is Dead – Long Live the Proliferation Network | Royal United Services Institute (rusi.org). Also, see the Khan Case presented by the FATF in their Proliferation Financing Report, page 62, at CHttpHandler.ashx (gov.gg).

[10] See Bahamas Customs' List of Prohibited and Restricted Imports and Exports.

[11] See "Identifying Proliferation Financing" document prepared by the Financial Reporting Authority, IDENTIFYING PROLIFERATION FINANCING (gov.ky).



3.4 Comparison between Money Laundering, Terrorist Financing and Proliferation Financing

ML, TF, and PF share several similarities, along with a few notable differences. They all pose significant jurisdictional risks that can be effectively mitigated through coordinated efforts by stakeholders. While they are similar, they also have distinct characteristics. A comparison of ML, TF, and PF can be found in the table below.

Comparison Between ML, TF, and PF

	Money Laundering	***Terrorist Financing***	***Proliferation Financing***
Definitions (Summarized)	ML is the process of concealing the origin of funds derived from criminal activities/predicate offences.	TF is the act of soliciting, collecting or providing funds with the intention of using them in support of terrorist activities.	PF is the act of providing funds which are used for nuclear, chemical, or biological weapons and their means of delivery and related materials in contravention of national laws or, where applicable, international obligations.
Origin of Funds	Funds are usually derived from criminal activity or predicate offences.	Funds can be derived from both legitimate and illegitimate sources.	Funds can be derived from both legitimate and illegitimate sources.
Transaction Red Flags	Focuses on suspicious transactions, outside of the norm for a customer's wealth.	Concerned with suspicious relationships between two parties who appear unrelated.	Focusing on detection of parties interacting with sanctioned persons, and the purchase of goods and services used in WMD production.
Destination of Funds	The money is ultimately returned to its source, after being legitimized through a series of transactions.	The money moves from the financier to the ultimate users of the funds: terrorists and terrorist organizations.	The money is sent from the state or individual to the broker or manufacturer of the goods and services needed for WMD development.

The key differences between ML, TF, and PF lie in the source and intended purpose of the funds. ML involves the process of legitimizing illegally acquired funds. These funds can then be employed for various

activities, including acquiring both legal and illegal goods and services. TF entails using funds, from legal or illegal sources, to support terrorist activities or organizations. Meanwhile, PF involves using funds from legal or illegal sources to acquire WMDs, which can then support proliferators in illicit acts, sometimes including acts of terrorism.

3.5 Identifying and Classifying Proliferation Financing Risks

Both public and private sector entities may encounter various PF risks. However, the FATF's definition of PF risks strictly refers to the potential breach, non-implementation, or evasion of the obligations of TFS.[12] When establishing counter-PF measures, it is essential to identify and assess additional PF risks that may exist. These risks can be categorized as either inherent or residual.

Inherent risks are associated with the nature of activities and the actors involved, prior to the implementation of specific countermeasures or policies. Understanding these risks is crucial for evaluating the effectiveness of control measures. In cases where no such measures are in place, it facilitates a better understanding of the impact of these risks on the jurisdiction or entity. The assessment of inherent risk levels can be based on various factors, including:

- *Proximity or links to sanctioned states or individuals* - The inherent PF risk level can rise based on the extent of business dealings with individuals associated with sanctioned entities.
- *Regulatory Gaps* – Loopholes in regulations aimed at the implementation of UNSCRs can create vulnerability for a jurisdiction and increase inherent risk.
- *The nature of exports and imports* – If a jurisdiction or customer is involved in the production or importation of dual-use goods, the inherent risk may increase.
- *Complexity of Services* – Institutions that offer complex products and services may have a higher level of inherent risk.
- *Customer base* – Institutions that onboard high-risk customers[13] might inherently face an increased risk of unintentionally engaging in PF activities.

Residual risks refer to the risks that remain after risk mitigation measures have been employed. These risks can emerge due to weaknesses or gaps in the execution or enforcement of countermeasures or policies. Nations and private sector entities that comprehend residual risks are better able to determine the effectiveness of their PF risk management efforts within their jurisdiction or business operations. A substantial level of residual risk may indicate the need for the jurisdiction or private sector entity to introduce supplementary controls. Some indicators that could imply a high level of residual PF risks for a jurisdiction include:

- *Limited implementation* – Countermeasures or policies may not be comprehensively implemented, leaving vulnerabilities that can be exploited by proliferation financiers.
- *Insufficient resources* – Jurisdictions or private sector entities may lack the necessary resources for complete implementation or enforcement of countermeasures or policies, resulting in exploitable gaps.

[12] As per the FATF's Guidance on Proliferation Financing Risk Assessment and Mitigation.
[13] An entity's customer base may be considered 'high-risk' due to a number of factors, including the geographical distribution of those customers.

- *Corruption* – Instances of corruption within jurisdictions or private sector entities can compromise the implementation or enforcement of countermeasures or policies, leaving potential vulnerabilities for exploitation.
- *Lack of coordination* – Inadequate coordination among jurisdictions or private sector entities can result in gaps or redundancies in countermeasures or policies.

Mitigation efforts that can be employed to address residual risks in a jurisdiction include:

- Regularly updating and adhering to current sanctions lists;
- Implementing a risk-based approach to customer onboarding and ongoing monitoring; and
- Enforcing a strong legislative framework for AML/CFT/CPF, including the ability to apply TFS obligations.

Residual risks underscore the importance of continuous monitoring, review, and improvement of countermeasures and policies to ensure their effectiveness and efficiency in addressing proliferation financing.

3.5.1 Performing a Proliferation Financing Risk Assessment

FATF's Recommendation 1 mandates both jurisdictions and private sector entities to perform a PF risk assessment. This enhanced understanding is essential for establishing a robust CPF framework.

A summary of the FATF's proposed stages of risk assessment is outlined in the table below:

Stages of Conducting a PF Risk Assessment	
Stage	***Explanation***
1. Preliminary Scoping Exercise	Determine the objectives, scope, and focus of the risk assessment, including consideration for public and private sectors, national CPF activities, and profiles for individuals and institutions.
2. Planning and Organization	It is encouraged to prepare a project plan and identify the relevant personnel from all stakeholders, including authorities and financial institutions.
3. Identification	It is encouraged to identify PF threats and vulnerabilities unique to the jurisdiction or private sector entity.
4. Analysis	Jurisdictions should analyze identified threats, vulnerabilities and the probability of potential occurrence. Consequences of those threats and vulnerabilities should also be considered.
5. Evaluation and Follow-Up	The analysis conducted should inform the jurisdiction or private sector entity of the priority risk areas that require urgent attention and mitigation.

Performing a PF risk assessment provides a comprehensive understanding of the exposure to threats, vulnerabilities, and consequences associated with PF.

- Threats – Threats include designated persons or entities with the potential to evade, breach, or exploit the failure to implement TFS. For instance, a customer engaged in importing dual-use goods for business operations could be a threat, as these goods are easily repurposed for proliferation activities.

- Vulnerabilities – Vulnerabilities are factors that can be exploited by threats, or that may facilitate the breach or evasion of TFS. These vulnerabilities can include weak legislative provisions and ineffectual operational controls, which make it easier for threats to operate.
- Consequences – Consequences occur when funds or assets are made available to designated persons and entities, allowing them to acquire WMDs or their means of delivery. Such consequences can result in loss of life due to the use of WMDs and the destabilization of commerce within the jurisdiction.

PF risk assessments may be conducted either as part of broader NRAs or specific stand-alone assessments, it may not require a stand-alone risk assessment if pre-existing risk assessment methodologies are adequate to incorporate PF risks.

4 Indicators of Potential PF-TFS Breach or Evasion

As previously indicated, PF risks refer to the breach, non-implementation, or evasion of TFS obligations. PF risks may emerge due to various factors, such as:

- **Risk of a potential breach or non-implementation of TFS:** This risk may materialize when designated entities and individuals access financial services, and/or funds or other assets, as a result of the following:
  - Delay in communication of designations at the national level;
  - Lack of clear obligations on private sector entities; and/or
  - Failure on the part of private sector entities to adopt adequate policies and procedures to address their proliferation financing risks.
- **Risk of evasion of TFS:** This risk may materialize due to concerted efforts of designated persons and entities to circumvent TFS.

The prior examples were not exhaustive, but risk indicators accompany each example. The presence of a risk indicator can imply or suggest the likelihood of unusual or suspicious activity. While a single indicator may not immediately warrant suspicion, it should trigger further monitoring. When multiple indicators are present, a more thorough examination becomes necessary.

The following risk indicators listed are not exhaustive and are based on the FATF's updated Guidance on Counter Proliferation Financing.[14]

4.1 Customer Profile Risk Indicators

- The customer provides vague or incomplete information about their proposed trading activities during onboarding and is reluctant to provide additional information about their activities when queried;
- The customer, (if an entity – its owners or senior managers), appears in sanctioned lists, negative news, or is subject to ongoing or past investigations or convictions;
- The customer has connections to a country that is of proliferation concern;

[14] See FATF's Guidance on Proliferation Financing Risk Assessment and Mitigation.

- The customer is involved in dealing with dual-use goods, goods subject to export control, or complex equipment for which they lack technical background, or which is incongruent with their stated line of activity;
- The customers or account holders have previously violated requirements under dual-use or export control regimes;
- The customer participates in complex trade deals involving numerous third-party intermediaries in lines of business differing from their business profile established at onboarding;
- A commercial business conducting transactions that suggest it is acting as a money-remittance business or a pay-through account, involving rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons;
- The customer is affiliated with a university or research institution and is involved in the trading of dual-use goods or goods subject to export control; and/or
- A customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or trade transactions.

4.2 Account and Transaction Activity Risk Indicators

- The transaction is carried out by or sent to a person or an entity ordinarily resident of or domiciled in a country of proliferation or diversion concern, such as DPRK and Iran;
- Transactions that involve items controlled under dual-use or export control regimes;
- Accounts or transactions involve possible companies with ownership structures that are not transparent, front companies, or shell companies;
- There are long periods of account dormancy followed by a surge of activity;
- The transaction reveals that the representatives of companies exchanging goods have definitive links, such as the same owners or management, physical address, IP address or telephone number, or they have co-ordinated their activities;
- Account holder conducts financial transaction(s) circuitously;
- Account activity or transactions involve associated financial institutions domiciled in a country with weak implementation of relevant UNSCR obligations and FATF Standards, or a weak export control regime (particularly relevant to correspondent banking services);
- Institutions' accounts receive sudden influxes of cash deposits followed by cash withdrawals;
- Transactions are made based on ledger[15] arrangements that prevent the need for frequent international financial transactions; and/or
- A personal account is used to purchase industrial items either under export control or unrelated to corporate activities or similar lines of business.

4.3 Trade Finance Risk Indicators

- Certain individuals and entities associated with DPRK are subject to asset freeze;[16]

[15] Ledger arrangements are conducted by linked companies who maintain a record of transactions made on each other's behalf. The linked companies will sometimes make transfers to balance the accounts in question.

[16] Individuals and entities listed in Annex I and II of the UNSCR 2087 (2013) OP 5(a), UNSCR 2094 (2013) OP 8, UNSCR 2270 (2016) OP 10, UNSCR 2321 (2016) OP3, UNSCR 2371 (2017) OP 18, and UNSCR 2375 (2017) OP 3, are subject to the asset freeze imposed in OP 8(d) of UNSCR 1718 (2006).

- A customer requests a letter of credit prior to approval of the account for use in a trade transaction for shipment of dual-use goods or goods subject to export control;
- Inconsistencies in information contained in trade documents and financial flows, such as names, addresses, and final destination;
- A freight forwarding firm is listed as the product's final destination on trade documents; and/or
- Wire instructions or payments from or due to entities not identified on the original letter of credit or other documentation.

5 Counter Proliferation Financing – Regulatory and Legal Framework

The Bahamas has established a robust legal and regulatory framework to combat proliferation financing and maintains close collaboration with international partners to implement and enhance its measures. This framework aligns with international standards, largely drawn from the United Nations and the FATF.

5.1 International Standards, Obligations and Sanctions Regimes

The Bahamas, as a United Nations member, has adopted several international instruments concerning CPF, including United Nations Security Council Resolutions and the FATF Recommendations as outlined in subsections 4.1.1 and 4.1.2, respectively.

5.1.1 United Nations Security Council Resolutions

The UNSC is tasked with the mission of identifying threats to and maintaining global peace and security. To achieve this mission, the UNSC may, in certain cases, employ measures like sanctions and other prohibitions through its UNSCRs on various jurisdictions. The primary UNSCRs pertinent to proliferation financing encompass UNSCRs 1540, 1718, and 2231.

Global Approach – UNSCR 1540 and its Successor Resolutions

UNSCR 1540 establishes comprehensive global measures for CPF. It prohibits engagement in any form of assistance to non-state actors,[17] which includes proliferators and terrorists, who aim to develop, acquire, manufacture, possess, transport, finance, transfer, or use nuclear, chemical or biological weapons and their means of delivery. Notably, this resolution does not require jurisdictions to freeze the assets of specific individuals or entities; instead, it focuses on regulating activities rather than imposing sanctions. Additionally, UNSCR 1540 mandates:

- Jurisdictions must establish and enforce robust laws and regulations that criminalize the possession and acquisition of WMDs, related materials, and their means of delivery.
- Implementation of domestic controls over nuclear, chemical, or biological weapons and their means of delivery.
- Jurisdictions are expected to uphold their commitments to CPF through multilateral agreements and cooperation.

[17] "Non-state actors" are individuals or entities, not acting under the lawful authority of any State in conducting activities, which come within the scope of UNSCR 1540. See Security Council Resolution 1540 - UNSCR.

Country-specific Approach – UNSCR 1718 and UNSCR 2231 and their Successor Resolutions

The UNSC has issued sanctions resolutions aimed at addressing proliferation activities in specific jurisdictions, notably the DPRK (UNSCR 1718) and Iran (UNSCR 2231). These resolutions include provisions that oblige jurisdictions to promptly freeze any assets linked to individuals or entities from the DPRK and Iran. The imposition of TFS related to PF, as outlined in these resolutions, forms the basis for FATF Recommendation 7 and its interpretive note.

5.1.2 Financial Action Task Force

The FATF employs a methodology for assessing technical compliance[18] with its recommendations and the effectiveness of AML/CFT/CPF systems. During mutual evaluations, the methodology includes minimal rating areas for CPF measures. The specific FATF recommendations that pertain to CPF measures are as follows:

- ***Recommendation 1***
  This recommendation requires countries and private sector entities to identify, assess, understand, and mitigate their proliferation financing risks concerning potential breaches, non-implementation, or evasion of TFS obligations referred to in Recommendation 7. In the context of R.1, proliferation financing risk refers strictly and only to the potential breach, non-implementation or evasion of the TFS obligations referred to in Recommendation 7.
  The source of proliferation financing risks would depend upon a number of factors as follows:

  a. Risk of a potential breach or non-implementation of TFS: This risk may materialize when designated entities and individuals access financial services, and/or funds or other assets, as a result, for example, of delay in communication of designations at the national level, lack of clear obligations on private sector entities, failure on the part of private sector entities to adopt adequate policies and procedures to address their proliferation financing risks (e.g. weak customer onboarding procedures and ongoing monitoring processes, lack of staff training, ineffective risk management procedures, lack of a proper sanctions screening system or irregular or inflexible screening procedures, and a general lack of compliance culture.
  b. Risk of evasion of TFS: This risk may materialize due to concerted efforts of designated persons and entities to circumvent TFS (e.g. by using shell or front companies, joint ventures, dummy accounts, middlemen and other fraudulent/sham intermediaries.

These assessments may be conducted as part of broader NRAs, or more specific stand-alone assessments. It should also be noted that a risk assessment to understand the potential risk of breach, non-implementation or evasion of PF-TFS, which is a process to be determined by the relevant country and private sector firms, may not necessarily require an entirely distinct or new methodological process, compared to how they have undertaken ML or TF risk assessments. It does not require a stand-alone risk assessment if pre-existing risk assessment methodologies are adequate to incorporate PF risks.

[18] Technical compliance refers to the implementation of the specific requirements of the FATF Recommendations, and the existence, powers and procedures of competent authorities.

- ***Recommendation 2***
  Countries are required to establish effective national cooperation and, when appropriate, coordination mechanisms to combat the financing of proliferation of WMDs.
- ***Recommendation 7***
  This recommendation obliges countries to implement PF-related TFS in accordance with UNSCRs.

In addition, the FATF assesses effectiveness based on 11 Immediate Outcomes, but only two of these outcomes specifically focus on CPF measures.

Overall Objective of PF Effectiveness Assessment: Financial systems and the broader economy are protected from the threats of the financing of proliferation.	
Immediate Outcome (IO)	***Description***
IO-1[19]	Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.
IO-11	Persons and entities involved in the proliferation of WMDs are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

The FATF has released several guidance reports regarding the countering of proliferation financing:

- *The FATF's Proliferation Financing Typologies Report*[20] assesses the threat of PF and identifies key issues and challenges in mitigating PF, including legal systems, public and private sector awareness, preventive measures, and investigation and prosecution.
- *The FATF's Report*[21] *on Combating Proliferation Financing*, which incorporates the UNSCRs on PF, focuses on policy development, and provides a blueprint for regulators and stakeholders in adopting policies to mitigate PF.
- *The FATF Guidance on Counter Proliferation Financing*[22], which provides guidance on the implementation of financial provisions of the UNSCRs to counter the proliferation of Weapons of Mass Destruction.
- Most recently, the FATF published its *Guidance on Proliferation Financing Risk Assessment and Mitigation*[23], which aims to assist jurisdictions with preparing PF risk assessments.

Key Elements of FATF PF Recommendations

Objective: This table summarizes the key elements in the guidance publications listed above.

Element	***Description***
Legal Frameworks	The FATF recommends that a jurisdiction's PF legal framework should take into consideration provisions for the criminalization of proliferation financing, asset forfeiture, financial investigations for proceeds and instrumentalities of proliferation financing, international cooperation, and export control systems.

[19] Updated in 2020 to include proliferation financing.
[20] 2008, FATF Proliferation Financing Typologies Report.
[21] 2010, FATF Report on Combating Proliferation Financing.
[22] 2018, FATF Guidance on Counter Proliferation Financing.
[23] 2021, Guidance on Proliferation Financing Risk Assessment and Mitigation.

Financial Institutions	The FATF suggests that financial institutions are to exercise vigilance over the activities of customers and potential customers. Jurisdictions should encourage FIs to incorporate a risk-based approach to monitor and assess the risk of PF as part of their established preventive measures and internal controls.
UNSCRs	The FATF encourages jurisdictions to adhere to relevant UNSCRs related to proliferation financing and TFS. It is suggested that jurisdictions implement UNSCRs 1540, 1718, 2231, and successor resolutions.
Risk Assessments	The FATF encourages that PF risk assessments are conducted at both the national level and private sector level, taking into consideration structural and sectoral vulnerabilities, and risk mitigation efforts by financial institutions and DNFBPs.

5.2 Domestic Obligations

To address domestic PF risks and challenges, competent authorities aided with the preparation of national legislation and policies that align with international CPF standards, recommendations, and obligations. This section provides an overview of the national CPF framework. Additionally, each financial services regulator has developed a framework specific to their sub-sectors, as outlined in the sectoral guidance.

Anti-Terrorism Act 2018 (ATA)

The ATA, along with subsequent amendments and regulations, establishes The Bahamas' framework that criminalizes terrorism, TF, proliferation of WMD, and PF. It also provides the necessary powers for the detection, prevention, prosecution, conviction, and punishment for such crimes.

Reporting Requirements

The ATA also mandates the implementation of the UNSCRs and designates the National Identified Risk Framework Coordinator as the person responsible for:

- Maintaining the list of designated entities; and
- Receiving and distributing UNSCRs to relevant authorities and industry participants.

According to the ATA, once financial institutions receive the list of designated entities,[24] the financial institution must immediately review their records and systems to determine whether the designated entity is connected by way of business. If so, the financial institution is mandated to immediately:

- Freeze all funds held in the designated entity's name and inform the designated entity; and
- Inform the FIU, the Office of the Attorney General, and other relevant competent authorities of its findings.

However, if a financial institution suspects that accounts are held in the name of a person suspected to be a designated entity, they are required to report this to the FIU. Non-compliance with reporting requirements may result in penalties, including fines and/or imprisonment.

[24] The term "designated entities" means individuals or entities and their associates designated as terrorist entities by the Security Council of the United Nations.

Financial Transaction Reporting Act 2018 (FTRA)

The FTRA, along with subsequent amendments and regulations, offers financial institutions and DNFBPs the legislative framework needed to address identified risks,[25] including proliferation financing. The table below outlines the key requirements of the FTRA.

Summary of FTRA Requirements for Financial Institutions and DNFBPs	
Requirements	***Description***
Risk Assessments	Financial institutions and DNFBPs must conduct a periodic risk assessment that identifies and assesses identified risks in aim to understand and mitigate the risks. This should be conducted, at a minimum, before the launch of a new product or developing technologies and when there is a major event in the management or operation of the firm.
Customer Due Diligence (CDD)	Financial institutions and DNFBPs must ensure that CDD is conducted before opening an account and entering into a correspondent relationship, and on an ongoing basis. These measures include the identification of beneficial owners.
Enhanced Due Diligence (EDD)	Financial institutions and DNFBPs must apply EDD measures in cases where a prospective customer or other business arrangement is connected with a high-risk jurisdiction.
Record Keeping	Financial institutions and DNFBPs must maintain all books and records of customers and transactions for a time period prescribed by law (no less than five years).
Internal Controls	Financial institutions and DNFBPs must prepare and implement policies and procedures to prevent activities of identified risks. This includes the designation of a compliance officer (CO).
Suspicious Transactions	Financial institutions and DNFBPs must report suspicious activities to the FIU via a suspicious transaction report (STR).

Suspicious Transaction Reporting

The FTRA outlines the procedures for reporting suspicious transactions and provides protection to those who report them:

- The GFSR's registrants, licensees, and supervised institutions can file STRs on the FIU's electronic filing platform "CaseKonnect".[26] All STRs, along with relevant supporting documentation, are completed, filed, and submitted by registered Money Laundering Reporting Officers (MLROs).
- Information that should be included in the STR are names, addresses, social security numbers, birth dates, driver's license or passport numbers, occupations, and phone numbers of all parties involved.
- It is important to disclose enough information to indicate the nature and reason for the suspicion.

For more information, visit the website, and address your concerns and applications to the Director of the FIU.

Proceeds of Crime Act 2018 (POCA)

The POCA, along with subsequent amendments and regulations, lays out the legislative framework for recovering proceeds from criminal activities and addressing identified risks, including proliferation

[25] As defined in Glossary.
[26] Available at https://fiuconnect.fiubahamas.bs/casekonnect/index.php?module=users/login.

financing. This Act establishes the Ministerial Council [27], the National Identified Risk Framework Coordinator, and the IRF Steering Committee. It also empowers law enforcement agencies, the Customs Department, and the Courts of The Bahamas in dealing with identified risks, including the ability to search, seize, and confiscate proceeds of crime associated with these activities.

Customs Management Act 2011

This Act provides for the control of exports and imports of goods that may be used for the development or acquisition of WMD or their delivery systems. It requires individuals or entities planning to export or import such controlled goods to obtain a license, which may come with specific conditions and restrictions aimed at preventing the proliferation of WMDs. Authorities are empowered to seize and detain any goods suspected of being intended for WMD development or acquisition, including their delivery systems.

As mentioned earlier, import and export controls are crucial elements of CPF measures, particularly concerning dual-use goods. In The Bahamas, the Customs Department, as mandated by the Customs Management Act, bears the responsibility for:

- Monitoring trade activities;
- Interdicting and confiscating contraband; and
- Protecting the nation's overall well-being and security by enforcing import and export restrictions and prohibitions.

The List of Prohibited and Restricted Imports and Exports is a valuable resource for identifying goods that may pose a high risk in the context of CPF.[28]

International Obligations (Economic and Ancillary Measures) Act 1993

This Act outlines the process for imposing economic sanctions and introduces ancillary measures to align with The Bahamas' international commitments. When the UNSC passes a resolution to impose sanctions on a specific person, entity, or jurisdiction, amendments or orders may be formulated to ensure that the UNSCR becomes full enforceable in The Bahamas.[29] The Minister of Foreign Affairs is responsible for the administration and enforcement of this Act.

UNSCRs are periodically transmitted to the individual tasked with maintaining the list of designated entities, which is the National Identified Risk Framework Coordinator. According to the Act, the Governor-General of The Bahamas is granted authority to put into effect orders or regulations aimed at limiting or prohibiting individuals or entities listed on the sanctions roster of the UNSC. The Governor-General also holds the power to issue directives for the seizure, freezing, or confiscation of property located in The Bahamas and held on behalf of such individuals and entities. Orders and Directions pertaining to sanctions have been enforced against individuals and entities associated with the Government of the Russian Federation, Al-Qaida, and ISIL, among others. These include:

[27] Has the responsibility of determining identified risks and make recommendations to update the Identified Risk Framework.
[28] List available at https://www.bahamascustoms.gov.bs/imports-and-exports/prohibited-and-restricted-imports-and-exports/.
[29] Information retrieved from Doing Business in The Bahamas: Overview.

- International Obligations (Economic and Ancillary Measures) (United States of America) (Unilateral Sanctions) Directions 2022;
- International Obligations (Economic and Ancillary Measures) (Democratic Republic of Korea) (Order) 2019;
- International Obligations (Economic and Ancillary Measures) (Iran) Order 2019;
- International Obligations (Economic and Ancillary Measures) (Iraq) (Order) 2018; and
- International Obligations (Economic and Ancillary Measures) (Afghanistan) (Order) 2018.

This Act requires Bahamian authorities and financial institutions to promptly freeze the funds, financial assets, and/or economic resources of individuals or entities listed in these Orders and Directions.

6 Sectoral Guidance

6.1 Central Bank of The Bahamas

The Central Bank of The Bahamas (the Central Bank) was established under the Central Bank of The Bahamas Act 1974, now superseded by the Central Bank of The Bahamas Act 2020 (CBA). Pursuant to the CBA, the Central Bank is entrusted with several key functions, including:

- Promoting stable monetary, credit and balance of payment conditions in order to safeguard the exchange rate regime and facilitate orderly and balanced economic growth;
- Contributing to the stability of The Bahamas' financial system by collaborating with domestic and foreign regulatory authorities;
- Regulating and supervising financial institutions; and
- Regulating and overseeing the issuance, provision and operation of payment instruments, whether they involve opening an account or not, which encompasses activities like issuing electronic money and other forms of stored value.

As part of its mandate, the Central Bank is tasked with the licensing, registration, regulation, and supervision of various financial institutions, including banks, trust companies, co-operative credit unions, non-bank money transmission service providers and their agents, and payment service providers. The Central Bank's oversight of these entities falls under the regulatory frameworks provided by the Banks and Trust Companies Regulation Act 2020 (BTCRA), the Bahamas Co-operative Credit Unions Act 2015,[30] and the Payment Instruments (Oversight) Regulations 2017.

All sectors that fall under the regulatory oversight of the Central Bank are required to adhere to the Central Bank's Guidelines on the Prevention of Money Laundering & Countering the Financing of Terrorism and Proliferation Financing (the AML/CFT/CPF Guidelines),[31] which were last revised 6 April 2023. These AML/CFT/CPF Guidelines provide guidance to supervised financial institutions regarding internal controls, customer onboarding, ongoing monitoring, and record-keeping, as mandated by relevant legislation, including:

[30] Including accompanying Regulations.

[31] Available at https://www.centralbankbahamas.com/bank-supervision/aml-cft-cpf-sfi-guidance-notes/guidelines-for-licensees-on-the-prevention-of-money-laundering-countering-the-financing-of-terrorism-and-proliferation-financing.

- Proceeds of Crime Act 2018 (POCA);
- Financial Transactions Reporting Act 2018 (FTRA); and
- Anti-Terrorism Act 2018 (ATA).

The Central Bank assesses compliance with these guidelines by conducting both off-site supervision and on-site examinations of supervised financial institutions, taking enforcement actions when necessary.

6.1.1 CPF Requirements

The entities under the Central Bank's regulation must comply with various laws, policies, and guidance that cover AML/CFT/CPF provisions. This sub-section provides a detailed breakdown of the requirements mandated by the Central Bank.

Onboarding Requirements for Prospective SFIs

In accordance with the *Guidelines for License Application*[32] and the *Banks and Trust Companies (License Application) Act*, SFIs must undergo a compliance due diligence verification process when applying for a license. To support the application, SFIs are required to provide at least the following:

- Due diligence documents to verify the identities of shareholders, directors, and officers;
- Information regarding supervisory functions, internal controls, risk management, and AML/CFT/CPF policies and procedures; and
- Details of any outsourcing agreements, if applicable.

Additionally, all SFIs are mandated to appoint a CO and the MLRO. The appointment of the MLRO must be approved by the Central Bank and registered with the FIU.

Verification of Customer Identity

Pursuant to the AML/CFT/CPF Guidelines (see also Section IV of AML/CFT/CPF guidelines), every SFI must undertake customer due diligence measures when initiating a business relationship with a facility holder or opening an account for them.

To fulfil these obligations, every SFI is required to:

- Verify the facility holder's identity using reliable, independent source documents, data or information; and
- Verify the identity of any person purporting to act on behalf of the facility holder and ensure that such a person is duly authorized for that role.

If an SFI cannot comply with the relevant CDD requirements or encounters circumstances in which it is not satisfied that the transaction it is or may be involved in is legitimate, the SFI:

- Must refrain from opening the account or establishing the business relationship;
- Must refrain from conducting the transaction;
- Must terminate the business relationship; and
- Should consider filing an STR with the FIU.

[32] Available at https://cdn.centralbankbahamas.com/download/023515700.pdf.

An SFI that intentionally opens an account, establishes a business relationship, carries out a transaction, or neglects to terminate a business relationship without meeting the requirements outlined in Sections 5 to 9 and 14 of the FTRA commits an offence. Upon summary conviction, the responsible individuals may face penalties, including a fine of up to $500,000, imprisonment for two years, or both. Legal entities could potentially be subject to a fine of up to $1,000,000.[33]

Monitoring of Business Relationships

SFIs must strictly adhere to the AML/CFT/CPF Guidelines when it comes to the ongoing monitoring of business relationships.

Once the initial identification procedures are successfully completed and the customer relationship is established, SFIs should maintain vigilance by monitoring the conduct of the relationship or account. The purpose of this monitoring is to ensure that the activities align with the business' stated nature when the relationship or account was initially established.

SFIs are tasked with implementing systems and controls for the ongoing monitoring of relevant account activities. The extent of this monitoring will vary based on the specific nature of the business. Accounts and customer relationships deemed higher risk will necessitate more comprehensive and frequent monitoring. This approach enables SFIs to stay alert and identify any noteworthy changes or transactions that deviate from the originally stated account purpose. Some potential areas of focus for monitoring include:

- Transaction type;
- Frequency;
- Amount;
- Geographical origin/destination; and
- Account signatories.

Internal Controls, Policies and Procedures

SFIs must establish clear roles and responsibilities to ensure that their policies, procedures, and controls, which are designed to deter criminals from using their services for ML/TF/PF, are not only put into practice but also consistently maintained and updated. This is crucial to ensure that SFIs fulfill their obligations as per AML/CFT/CPF laws and meet the requirements outlined in the AML/CFT/CPF Guidelines. These requirements include, but are not limited to:

- Verifying customer identities;
- Assessing customer risk levels;
- Monitoring ongoing relationships and transactions;
- Adapting to new products, practices, and technological advancements;
- Adhering to sanctions in line with the relevant UNSCRs;
- Appointing a CO and MLRO;

[33] See section 11 of the FTRA.

- Reporting suspicious transactions;
- Upholding "know your employee" standards and expectations; and
- Implementing internal controls in a group of affiliated entities.

In addition, SFIs are expected to perform a self-risk assessment that encompasses an evaluation of their inherent ML/TF/PF risks, the control mechanisms in place to mitigate those risks, and the implementation of supplementary measures to manage residual risks where necessary. The Central Bank expects risk assessments to include the following:

- Clear risk assessment methodology;
- Defined risk appetite and risk tolerance;
- Identification and evaluation of inherent risks;
- Identification and assessment of control measures;
- Development of corrective action plans, where applicable; and
- Evaluation of residual risk.

SFIs are required to monitor and update their risk assessments on an ongoing basis.

SFIs should utilize the ML/TF/PF Risk Assessment Guidance Notes[34] to identify and rectify gaps within their risk assessment frameworks using a proportionate and risk-based approach.

Record Keeping

Sections 15, 16 and 17 of the FTRA mandate that SFIs maintain records related to customer identification and transactions. These records serve as crucial evidence in investigation into money laundering or terrorist financing, particularly when individuals involved employ intricate transaction networks designed to obscure the audit trail.

The records kept by SFIs about their customer relationships and transactions should meet the following criteria:

- Full compliance with legal requirements;
- Accessibility for competent third parties to assess the SFIs adherence to AML/CFT/CPF policies and procedures;
- The ability for the SFI to meet court orders and inquiries from relevant authorities;
- The capacity to reconstruct any wire transactions conducted through the SFI, with comprehensive information on both the payer and payee, including identity verification documentation; and
- A mandatory retention period of five years from the execution of the transfer for all relevant information, as stipulated by the originating financial institution.

Retention Period and Record Format

To facilitate the verification of an individual's identity, SFIs must maintain records that allow for easy identification of the evidence used for this verification by the FIU. These records encompass identify

[34] Available at https://www.centralbankbahamas.com/viewPDF/documents/2023-08-25-18-03-33-MLTFPF-Risk-Assessment-Guidance-Notes-June-2023-Header-Update.pdf.

verification for facility holders and beneficial owners, as well as account files, business correspondence, and the outcomes of any analysis conducted. It is mandatory for SFIs to retain these records for a minimum of five years, starting from the date when an individual no longer holds facility status.

In keeping with best practices, the point at which an individual ceases to be a facility holder is determined by the following criteria:

- The completion of a one-off transaction or the final transaction in a series, or
- The termination of a business relationship, which includes the closure of the account(s).

In cases where formal steps to conclude a business relationship have not been taken, but a period of five years has passed since the date of the last transaction, investigation, or prosecution of any offense, the five-year retention period commences from the date of the final transaction.

These records must be stored in an accessible and convertible format, such as original documents, microfiche, or computer disks. This storage method should also remain in compliance with the FTRA 2018 and the Evidence Act 1996 to ensure admissibility of computerized evidence.

Education and Training

In line with the AML/CFT/CPF Guidelines and the Financial Intelligence (Transactions Reporting) Regulations 2001, SFIs are obligated to establish ongoing AML/CFT/CPF training programs. They must provide suitable training to relevant employees, directors, and officers at least once per year. This training is crucial to maintain their awareness of:

- All AML/CFT/CPF policies and procedures, which includes aspects like identification, record keeping, the recognition and handling of unusual or suspicious transactions, as well as internal reporting; and
- Relevant AML/CFT/CPF legislation and supervisory guidance notes that apply to their responsibilities.

Enforcement Matters

Pursuant to section 57 of the FTRA, the Central Bank has power to levy Administrative Monetary Penalties (AMPs) against SFIs or individuals, including employees, directors or senior managers of an SFI. These penalties are primarily intended to uphold high standards of regulatory conduct by deterring any contraventions of the FTRA or other relevant AML/CFT/CPF laws. In cases involving SFIs, the Central Bank can impose penalties of up to $200,000, while individuals may face penalties of up to $50,000.00.

The Central Bank's schedule of penalties is set out in the *Administrative Monetary Penalties for Supervised Financial Institutions under The Bahamas' Anti-Money Laundering and Terrorist Financing Regime*.[35] It provides a summary of circumstances warranting penalties and the corresponding monetary amounts.

[35] Available at https://www.centralbankbahamas.com/viewPDF/documents/2021-02-05-12-17-45-AMP-Guidance-Note-revised-Nov.-2020.pdf.

In addition it is important to note that offences under the POCA may result in prison sentences ranging from seven to twenty years upon summary conviction (see section 15 of the POCA).

6.2 Securities Commission of The Bahamas

Established in 1995 by the Securities Board Act[36], the Securities Commission of The Bahamas (SCB) is a financial services regulator committed to developing a growing, vibrant, competitive financial services sector. The SCB is given broad powers under its legal and regulatory framework to promote fairness and integrity in The Bahamas' capital markets. It also supervises and regulates the securities and capital markets, investment funds and investment fund administrators, digital asset businesses and activities, carbon credit trading, and financial and corporate service providers. Accordingly, participants in any of the aforementioned are required to be licensed or registered under at least one administered legislation. The legislative framework that supports the SCB in its duties includes, but is not limited to:

- The Securities Industry Act 2024 and The Securities Industry Regulations 2012;
- The Investment Funds Act 2019, Investment Funds Regulations 2020 (and the associated amendments thereto), and the Investment Condominium Act 2014;
- The Financial and Corporate Service Providers Act 2020 and The Financial and Corporate Service Providers (General) Regulations 2020;
- Digital Assets and Registered Exchanges Act 2024; and
- The Carbon Credit Trading Act 2022.

A summary of the broad powers of the SCB include, among others:

- Regulating and governing the capital markets, securities and investment fund businesses, digital asset businesses, and carbon credit exchanges, etc.;
- Entering the premises of registrants and licensees to conduct examinations or inspections;
- Taking enforcement action against any person for failing to comply with applicable laws;
- Granting, refusing to grant, or revoking licenses and registrations;
- Making recommendations regarding regulations to the Minister of Finance;
- Implementing rules to supplement the regulatory framework, as necessary; and
- Doing all things and taking all actions which may be necessary or expedient or which are incidental to the discharge of any function of power of the SCB.

In addition to requiring registrants and licensees to follow national AML/CFT/CPF requirements, the SCB also provides sector-level Rules that encompass CPF provisions, namely:

- The Securities Industry (Anti Money Laundering and Countering the Financing of Terrorism) Rules 2015;
- The Financial and Corporate Service Providers Act (Anti Money Laundering and Countering the Financing of Terrorism) Rules 2019; and
- The Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering Financing of Terrorism and Countering Financing of Proliferation) Rules 2022.

[36] Repealed and replaced by the Securities Industry Act 1999 and later the Securities Industry Act 2011 and Securities Industry Act 2024.

These Rules provide targeted provisions for sector stakeholders and in some cases may be stricter than those at the national level, previously outlined in section 4 of these Guidelines.

6.2.1 CPF Requirements

The sectors regulated by the SCB are guided by a wide array of legislation, policies, and guidance that encompass AML/CFT/CPF provisions, including legislation enacted at the national level and sector level. Elements of the legislation that strengthen the SCB's CPF framework include onboarding requirements, ongoing requirements, examination procedures, and enforcement-related matters.

Onboarding Requirements

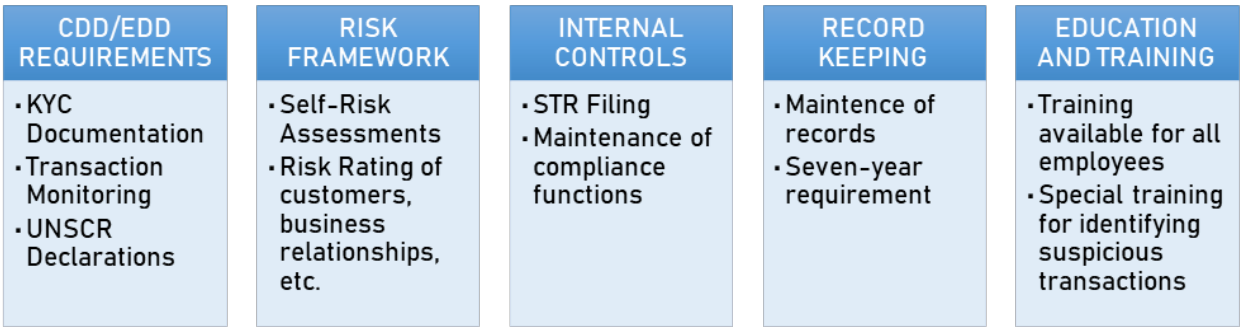
During the SCB's registration process, prospective registrants/licensees are subject to a background check that encompasses CPF measures, which may include revision of:

- KYC documents on all official Directors and Officers;
- Supervisory functions, internal controls, risk management, and AML/CFT/CPF policies and procedures; and
- Outsourcing agreements, if applicable.

Additionally, all registrants and licensees are mandated to appoint both a CO and MLRO and register them with the SCB.

Ongoing Requirements

The SCB administers the FTRA for all its registrants and licensees; meaning, it ensures that all its registrants and licensees adhere to the provisions of the FTRA. This includes adherence to all CPF provisions. Additionally, as previously mentioned, SCB requires all registrants and licensees to adhere to the provisions of applicable sector-level AML/CFT/CPF Rules. Common ongoing requirements expected by the SCB are:



- ***Due Diligence Requirements.*** Registrants and licensees are required to implement CDD measures, which applies to its risk-rating framework. At a minimum, firms are to ensure that all customers are appropriately identified and sufficient information and documentation is obtained. A customer's identity must be verified prior to customer onboarding and prior to an occasional transaction involving a cash amount over the threshold allowed under the Financial Transactions

Reporting (Wire Transfer) Regulations. To assist with verifying customers, the registrant or licensee may collect either:

- Original documents;
- Certified copies of documents where submission of original documents is impractical or impossible;
- Independent and reliable source documents, data or other information (whether or not electronically sourced) which sufficiently verifies a customer's identity; or
- Photographed or scanned copies of identifying documents provided that the registrant has adequate internationally recognized tools to verify the authenticity of the documents.

It is also required that registrants and licensees implement EDD measures for high-risk customers, business relationships, and transactions.

Once the verification procedures are concluded and a relationship has been established, it is required that the registrant or licensee continue to:

- Monitor the conduct of the business relationship periodically; and
- Ensure, on an ongoing basis, that the business relationship is consistent with the risk profile and nature of the business stated when the relationship was established.

As it relates specifically to PF risks, the SCB requires registrants and licensees to prohibit customer relationships of persons and entities that are present on various sanctions lists prepared by the UNSC. Periodically, the SCB receives UNSCR declarations from the National Risk Coordinator that outlines a list of persons or entities that should be prohibited from conducting business in The Bahamas. These declarations are then sent to registrants and licensees, and it is expected that these are completed and submitted to the SCB within the timeline stipulated. If a registrant or licensee finds that the prohibited person or entity is an existing customer or involved in business relationships, it is expected that this be made known on the declaration and that the relationship is immediately severed.

- ***Risk Framework.*** Registrants and licensees are required to approve and implement a risk rating framework that assesses various components of the business, including the risk profile of:
  - Every customer;
  - Its dealings in each jurisdiction/country that it operates;
  - Its own business practices, products, services, transactions, and delivery channels;
  - Non face-to-face business relationships, including the nature and extent of risks involved; and
  - The nature and extent of risks related to its business activities that allow customers to receive payments from unknown or unconnected third parties.

Additionally, registrants and licensees are required to perform a self-risk assessment to evaluate its own risk for vulnerability to breaches of the FTRA, the POCA, and the ATA. It is expected that this risk assessment be conducted:

- Prior to the launch of a new or existing product or business practice;

- Prior to the use of new, existing, or developing technologies; and
- Where the registrant/licensee is a part of a group, when there is a major event or development in the management or operation of the group.

- ***Internal Controls.*** Registrants and licensees are required to implement internal control policies and procedures that constitute an AML risk-based approach to monitoring facilities. This includes an overall risk management framework for the prevention, detection, and disclosure of identified risks associated with ML, TF, and PF. It is expected that these internal controls be updated, as necessary, on an ongoing basis. It is also expected that each registrant and licensee implement a compliance program with a registered CO and MLRO that will assist the firm with maintaining its mandated compliance functions. This compliance program must also include policies and procedures in relation to suspicious transaction reporting.

- ***Record Keeping.*** Registrants and licensees are required to maintain records and documents in relation to customers and business relationships for a period of seven years from the date that the customer ceases to be a facility holder. The types of record maintained must enable:
  - Competent third parties to assess the registrant's compliance with AML/CFT/CPF policies and procedures;
  - Transactions effected through the registrant to be reconstructed;
  - The registrant/licensee to satisfy court orders or enquiries from the SCB or appropriate authorities; and
  - The identification of customers.

- ***Education and Training.*** Registrants and licensees are required to ensure that all employees are adequately trained, on an ongoing basis, on:
  - The policies and procedures put in place to detect and prevent ML, TF, and PF, including those for the identification, record keeping, detection of unusual and suspicious transactions and internal reporting; and
  - The AML/CFT/CPF legislative framework.

Note: This section presents a summary of requirements. For full scope of requirements, please review:

- The Securities Industry (Anti Money Laundering and Countering the Financing of Terrorism) Rules 2015;
- The Financial and Corporate Service Providers Act (Anti Money Laundering and Countering the Financing of Terrorism) Rules 2019; and
- The Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering Financing of Terrorism and Countering Financing of Proliferation) Rules 2022.

Examination Procedures

One of the powers imparted to the SCB via its legal and regulatory framework is the power to conduct examinations. Examinations typically involve inspecting a registrant or licensee's business practices,

internal controls, and overall compliance with applicable legislation, including AML/CFT/CPF requirements. There are, broadly, three main types of inspections:

Types of Examinations	
Examination Type	***Brief Explanation***
1. Routine Examinations	On-site or off-site examinations, where the frequency is based on the registrant's or licensee's assessed level of risk. Areas inspected include AML/CFT/CPF procedures, business conduct, solvency analysis, compliance with registration requirements, et al.
2. For Cause Examinations	Inspections conducted with reason, outside of the normal course of the SCB's examination cycle. Credible information on improper conduct provided to the SCB may create a situation where an inspection of a licensee or registrant's premises and business operations is urgently required. This may include potential AML/CFT/CPF infractions.
3. Thematic Examinations	Inspections conducted to determine a registrant or licensee's compliance in a particular area of interest for SCB. They are differentiated from for cause examinations in that thematic examinations are typically not a result of credible information concerning dubious behavior. Instead, they represent an opportunity for SCB to gather additional information regarding its licensees' ability to comply with standards of best practice in a particular area, both locally and internationally.

In cases where there are violations of relevant legislation found during the course of the examination, the registrant or licensee may receive fines, license suspension/revocation, or other enforcement consequences commensurate with the nature of the violation.

AML/CFT/CPF Testing

The examination of licensees and registrants provides the opportunity to gain reasonable assurance of compliance with relevant AML/CFT/CPF legislation. Many of the areas reviewed by SCB during the course of an examination are AML/CFT/CPF focused and may include, among others:

- Performing reviews to determine whether a risk management framework has been implemented in accordance with the FTRA 2018, in addition to an AML risk-based approach to monitoring facilities;
- Review of the processes, policies, and procedures surrounding the handling of client complaints;
- Ensuring the CO and MLRO for the organization are registered with SCB and FIU, as mandated;
- Reviewing AML/CFT/CPF policies and procedures;
- Reviewing the customer onboarding process for the organization, as well as ensuring ongoing monitoring is conducted, and appropriate up-to-date documentation is retained;
- Random sampling and testing of CDD and customer risk ratings, and review of the procedures surrounding the customer risk rating determination process;
- Testing whether employees of the organization are regularly trained in recognition of ML/TF/PF, and evaluating whether staff are appropriately qualified and experienced for the level of their responsibility within the organization;
- Performing reviews to determine whether the registrant maintains adequate supervisory personnel appropriate to the nature and size of the firm.

- Ensuring policies and procedures regarding STRs are implemented, and that employees are aware to whom they should be reported;
- Testing a sample of transactions conducted by the organization, and reviewing its policies and procedures surrounding large transactions;
- Reviewing policies and procedures surrounding the investigation and reporting of any potential suspicious activities to the FIU via the submission of an STR by the CO/MLRO;
- Reviewing the autonomy of the role of the MLRO within the organization to determine whether the MLRO has sufficient seniority within the organization, and evaluating the level of independence of the MLRO such that the MLRO's assessment of any transaction may not be compromised by senior management of the entity;
- Obtaining a list of jurisdictions with which the registrant or licensee does business, and relevant declaration letters to corroborate compliance with sanctions lists;
- Testing record keeping procedures to gain reasonable assurance that registrants and licensees are maintaining records (including discontinued files due to closed customer relationships) in compliance with legislative requirements; and
- Reviewing policies and procedures surrounding politically exposed persons (PEPs).

Enforcement Matters

SCB requires all of its registrants and licensees to comply with both the FTRA and the POCA. Penalties against both include imprisonment or fines, and the SCB has the right to further impose administrative breaches up to $200,000 for entities in breach, or in the case of an individual, up to $50,000. The SCB may also impose a monetary penalty or otherwise require another form of sanction and/or remediation if it considers the infraction warrants it. The schedule of administrative penalties may be found on the SCB's website.[37]

6.3 Insurance Commission of The Bahamas

The Insurance Commission of The Bahamas (ICB) is the regulatory body responsible for overseeing and enforcing insurance laws and regulations in The Bahamas. Its mandate is to protect policyholders and ensure the solvency of insurance companies operating in and through The Bahamas. The ICB is primarily governed by the Insurance Act 2010, which provides for the regulation and supervision of insurance companies and intermediaries. The Act sets out the licensing requirements for insurers, the standards they must meet and the penalties for non-compliance.

The ICB's powers include:

- Licensing and registration of insurers and intermediaries – the ICB is responsible for granting and renewing licenses to insurers and intermediaries that meet the regulatory requirements.
- Supervision and monitoring of insurers and intermediaries – the ICB has the power to monitor the activities and financial performance of insurers and intermediaries to ensure compliance with regulatory requirements.

[37] Available at www.scb.gov.bs.

- Enforcement of insurance laws and regulations – the ICB has the power to investigate and take enforcement action against insurers and intermediaries that violate insurance laws and regulations.
- Establishment of prudential and conduct standards – the ICB has the power to establish prudential and conduct standards for insurers and intermediaries, such as capital requirements, reserve levels, and customer protection measures.
- Approval of insurance products and services – the ICB has the power to approve insurance products and services to ensure they comply with regulatory requirements.
- Collaboration with international regulatory bodies – the ICB collaborates with international regulatory bodies to ensure that the industry in The Bahamas meets international best practices and standards.

In addition to its regulatory responsibilities, the ICB also has a role in the country's AML/CFT/CPF, including the FTRA, the POCA, and the ATA. The AML/CFT/CPF framework is outlined in the ICB's Anti-Money Laundering/Countering the Financing of Terrorism/Prevention of Financial Crimes Guidelines for Insurance Companies (ICB AML Guidelines).[38] The ICB AML Guidelines provide guidance on how to comply with AML/CFT/CPF laws and regulations. The ICB supervises life insurance companies through a combination of on-site and off-site examinations, education, training, and awareness programs. In addition, periodic notices and guidelines are issued to supplement the ICB's AML Guidelines.

Onboarding Requirements

The ICB supervises all licensees of the insurance industry and routinely assesses compliance with AML/CFT/CPF laws. The assessment includes:

- CDD to identify and verify the identity of customers, their beneficial owners, and any politically exposed persons (PEPs);
- Assessing and documenting the risk of money laundering, terrorist financing, and other financial crimes associated with the customer and the proposed business relationship;
- Establishing and verifying the identity of intermediaries, such as agents and brokers, involved in the business relationship.

Ongoing Requirements

Licensees must ensure that there are procedures/practices in place for the five operational areas of an insurer's activities, particularly:

- Verifying/identifying of customers;
- Maintaining customer verification and transaction records;
- Reporting suspicious transactions to the FIU;
- Assigning a CO and MLRO; and
- Reviewing internal procedures for training personnel on money laundering detection and prevention as required.

[38] Available at https://insurancecommissionbahamas.com/wp-content/uploads/2019/10/AML-CFT-PF-Guidelines-for-Insurance-Companies-Sept-2018-1.pdf.

Verifying Details and Documentary Evidence Procedures

Licensees of the ICB have a general duty to verify the identity of those with whom they do business. Financial institutions and DNFPBs must verify that they are dealing with a legitimate person (natural, corporate or legal). When possible, the prospective customer should be interviewed personally.

Life insurance companies should verify identity in the following circumstances:

- ***Existing Facility Holders.*** All existing facility holders of record who are above the established threshold must verify the identity of their customers. Where doubt arises in relation to any facility holder during the business relationship, a verification of the facility holder must be done.
- ***New Facility Holders.*** Before establishing a new facility, all persons authorized to operate the facility must be verified. Also, before someone new is added as a facility holder to an existing facility, that person must be verified.
- ***Certain occasional transactions exceeding $15,000.*** Individuals who seek to conduct a transaction with a life insurance company via existing facilities involving cash exceeding $15,000 (an occasional transaction) and the transactor is not a customer in relation to any financial intermediary services provided by the insurance company or is conducting the transaction on behalf of someone who is not.
    - Where a person, who cannot be regarded as a customer holder, seeks to conduct an occasional transaction in relation to any facility, that person must be verified before such transaction is permitted.
    - Where a person, who is also not a customer in relation to the subject facility seeks to conduct **an occasional transaction (cash) on behalf of another** who is also not a facility holder of the firm. In addition to the transactor being verified the person on whose behalf he is acting must also be verified.
    - Where a customer facility holder seeks to use his own facility, which is provided by the life insurance company to conduct occasional transactions on behalf of others (most commonly the case for intermediaries such as attorneys) must be verified.
    - Where structuring[39] of an occasional transaction is suspected to be taking place.

Obligations where Unable to Complete CDD

Where the insurance company is unable to complete the CDD/KYC verification procedures, it must not commence a business relationship or perform the transaction, or must suspend or terminate the business relationship until sufficient information can be obtained. The company should consider filing an STR concerning the customer.

[39] Structuring transactions as a means of avoiding having to provide verification evidence is a practice known in money laundering scheme. Structuring is also referred to as "linked" transactions or "smurfing" and present special challenges for verification prior to the transaction being conducted.

Tipping Off

Where an insurance company becomes suspicious of ML/TF/PF activities while conducting CDD, they should consider the risk of tipping off. If, when performing CDD, there is a reasonable belief that the customer may be tipped off during the process, the insurance company may elect to not pursue the CDD process. A STR should still be filed. Insurance companies should ensure that their employees are made aware of these issues.

Documentary Evidence

There must be sufficient documentary evidence to establish the identity of the client/customer on record, as part of the due diligence process. This is for every facility or occasional transaction that has been verified for low, medium, or high-risk customers. Regulations 3, 4, and 5 of the Financial Transactions Reporting Regulations 2018 (FTRR) provide a list of mandatory documentation and information to verify identity, as well as additional information that may be used to further establish the identity of a person that must be verified. Determining any additional information that may be required for high-risk customers should be documented in the company's enhanced due diligence procedures for high-risk customers.

Verification Information for Individuals

The following evidence must be on record for every facility or occasional transaction that must be verified:

- Full and correct name;
- Permanent address;
- Date and place of birth;
- Purpose of the facility;
- Potential activity involving the facility; and
- Written confirmation that all credits to the facility are and will be beneficially owned by the facility holder, except in the case of a facility that will be an intermediary facility. Verification of beneficial owner should be completed separately.

Additional Identification (Non-resident Customers)

A social security, social insurance or national insurance number is a useful means to identify non-residents. Licensees are encouraged to record such information, as part of the customer profile.

Verifying Information for Corporate Bodies (Legal Persons and Legal Arrangements)

Mandatory requirements for verifying corporate entities, including those that are non-profit organizations (NPOs), whether incorporated in The Bahamas or elsewhere include:

a. Certified copy of the Certificate of Incorporation;
b. Certified copy of the Memorandum and Articles of Association;
c. Notification of perspective Board of Directors;
d. Resolution from the Board of Directors authorizing the opening of the account and conferring authority on the person who will operate the account;
e. Names of senior management holders;

f. Location of the registered office or agent and, the principal place of business;
g. Documentary evidence when unable to complete standard CDD;
h. Confirmation that the corporate entity has not been struck off the business register, or is not in the process of being wound up;
i. Written confirmation that all credits to the facility are and will be owned by the customer corporate entity except in the case of a facility that will be an intermediary facility in which case the beneficial ownership identification information will have to be provided separately;
j. Names and addresses of all beneficial owners (the obligation to verify the identity of beneficial owners shall only extend to those with at least 10% controlling interest in the corporate entity); and
k. The purpose and intended nature of the business relationship, products and/or services provided.

The requirements in c, d, e, f, and j should be regularly updated. In addition to the requirements outlined above, the following information and documents may also be used to support verification of a corporate entity:

- List of shareholders;
- The potential parameters of the facility including size (for investment and custody accounts);
- Balance ranges (in the case of deposit accounts and the expected transaction volume of the account);[40] and
- Such other official document and other information as is reasonably capable of establishing the ownership and control structure of the corporate entity.

Insurance providers must take reasonable measures to determine the natural persons who control the management of the corporate entity and its ownership structure. Natural persons must be willing to cooperate with competent authorities, providing basic information, particularly on the beneficial ownership.

6.3.1 Categorization and Mitigation of Risk

The ICB requires that all its licensees conduct a risk assessment. This risk assessment should determine a customer's or a product's/service's risk category, whether low, medium, or high. Licensees must also ensure that their procedures include mitigation mechanisms. These mechanisms involve identifying and applying CDD/KYC policies and procedures to mitigate money laundering risk of particular customers, products or services identified during the assessment process.

Risk Identification

Licensees must collect the following information for all customers to their satisfaction. This information will enable licensees to determine their level of AML/CFT/CPF risk.

Who is the customer?	Is there public information that associates this person with any known ML/TF/PF activities?

[40] References to "account" in relation to verification evidence in the case of a life insurance company should be construed to mean the facility or financial intermediary service that is being provided to that customer facility.

What is the customer's business?	Is this customer's occupation or business activities commonly linked to ML/TF/PF activities?
Where is the customer located?	Does the customer's jurisdiction apply globally acceptable AML/CFT/CPF standards?
Where does the customer transact business?	Does the jurisdiction where this customer transacts business apply adequate AML/CFT/CPF standards or is it commonly linked to ML/TF/PF activities?
What products and services does the customer require?	Do the products and services provided to the customer offer the anonymity and movement of funds commonly linked to ML/TF/PF activities?

A similar assessment of the inherent risks associated with products and services should also be conducted. Customers, products, and services should be categorized based on the degree of money laundering and terrorist financing risk they pose to the licensee.

Risk Characteristics

When developing an overall risk framework, it is critical to determine the potential money laundering and terrorist financing risks posed by a customer or a category of customers. In determining the risk profile of any customer, licensees should consider the following factors:

- Significant and unexplained geographic distance between residence or business location of the customer and the location of the insurer's representative;
- Frequent and unexplained movement of funds between financial institutions in various geographic locations;
- Customers that are legal persons whose structure makes it difficult to identify the ultimate beneficial owners or controlling interests;
- Customers who seek or accept very unfavourable account/policy/contract provisions or riders.
- Charities and other "not for profit" organizations that are not subject to monitoring or supervision (especially those operating cross-border).
- "Gatekeepers" such as accountants, lawyers or other professionals holding accounts/policies/contracts at an insurance company, acting on behalf of their customers, and where the insurance company places unreasonable reliance on the gatekeeper.
- Customers who are Politically Exposed Persons (PEPs) and close associates of PEPs.
- Customers where the beneficial owner of the contract is not known (i.e. certain trusts).
- Customers who are introduced through non-face to face channels.
- Customers who use unusual payment methods, such as cash, cash equivalents (when such a usage of cash or cash equivalents is, in fact, unusual), or structured monetary instruments.

- Customers who seek early termination of a product, especially at a cost to the customer, or where payment is made by, or the refund check is directed to, an apparently unrelated third party.
- Customers who transfer the benefit of a product to an apparently unrelated third party.
- Customers who show little concern for the investment performance of a product, but a great deal of concern about the early termination features of the product.
- Customers who are reluctant to provide identifying information when purchasing a product, or who provides minimal or seemingly fictitious information.

6.3.2 Record Keeping Procedures

There is a statutory requirement that insurance companies retain their records concerning customer identification and transactions for use as evidence in investigations into money laundering and terrorist financing. Often, the only significant role a financial institution plays in an investigation is providing records, particularly where the money launderer or person financing terrorism used a complex web of transactions in an attempt to confuse the audit trail.

Where there is a statutory obligation to keep records, copies are sufficient, unless the law specifically states otherwise. Insurance companies must satisfy themselves that copies are reproductions of the original documentation. The files should indicate where the originals can be located. These files, which are prepared and maintained as records of the customer relationship and transactions, should be such that:

- Requirements within legislation are fully met;
- Competent third parties will be able to assess the firm's observance to money laundering policies and procedures;
- Any transactions effected via the firm can be reconstructed; and
- The firm can satisfy any enquiries or court orders from the appropriate authorities to disclose relevant events.

These documents can be the original documents, or stored on microfiche, computer disk, cd rom, or in other electronic forms.

Retention Period

Records that relate to verifying the identity of any person must be kept for a period not less than five years after verification. Records relating to the verification of the identity of facility holders must be retained for five years after the person ceases to be a facility holder. In keeping with best practices, the date when a person ceases to be a facility holder is the date of:

- The carrying out of a one-off transaction or the last in the series of transactions;
- The ending of the business relationship, i.e., the closing of the facility; or
- The commencement of proceedings to recover debts payable on insolvency.

Where formalities to end a business relationship have not been undertaken, but a period of five years has elapsed since the date when the last transaction was carried out, then the five-year retention period begins on the date of the last transaction was completed. Records that relate to the verification of identity for any transaction conducted through a facility of an intermediary must be kept for a period of not less

than five years after the intermediary ceases to be a facility holder. All records related to ongoing investigations must be retained until it is confirmed by the FIU or local law enforcement that the case has been closed.

Minimum Retention Period

Records of suspicion that were raised internally with the MLRO but not disclosed to the authorities should be retained for at least five years from the date of the transaction. Records of suspicions, which authorities have advised are of no interest, should be retained for a similar period. Similarly, records of an insurance company's inquiry into unusual activity should be retained for a minimum of five years following the termination of the business relationship or after the date of the occasional transaction. Licensees should also retain any analysis conducted or considered.

Transaction records

Transaction records (both domestic and international) must be kept for a minimum period of five years after the transaction has been completed, subject to the extended requirements where the records relate to an ongoing investigation then they must be retained until it is confirmed by the FIU or local law enforcement that the case has been closed.

Transaction records to be kept must include the following information:

- Nature of the transaction;
- Amount of the transaction, and the currency in which it was denominated;
- Date on which the transaction was conducted;
- Parties to the transaction;
- Where applicable, the facility through which the transaction was conducted, and any other facilities (whether provided by the insurance company) directly involved in the transaction; and
- All other files and business correspondence and records connected to the facility.

6.4 Compliance Commission of The Bahamas

The Compliance Commission of The Bahamas (CC) is a statutory authority established under the FTRA. The CC exists for the express purpose of ensuring that financial institutions within their remit,[41] comply with the provisions of the FTRA.

The CC commenced its operation on 1 January 2001 as the anti-money laundering regulatory authority for DNFBPs[42] inclusive of real estate agents and brokers, land developers, dealers in precious metals, precious stones and pawnshops, lawyers, accountants, persons acting in the capacity of trustee and designated government agencies.

[41] As set out in section 32(2) and subsequently in sections 3 and 4 of the FTRA.
[42] Specified in section 4 paragraphs a, b, c, e, f, g, h, i, j, and k of the FTRA 2018.

The CC falls within the responsibility of the Ministry of Finance. There are several key pieces of legislation relevant to DNFBPs, including the Anti-Terrorism Act, Financial Transactions Reporting Act, and the Proceeds of Crime Act.[43]

6.4.1 CPF Obligations for DNFBPs

The objectives of UNSCRs is to ensure that proliferators are identified, deprived of economic resources, and prevented from raising, moving and using funds or other assets for the financing or proliferation.

To ensure that all DNFBPs are aware and updated on all PF-related information the CC sends out, via email, all sanction updates. Registrants are required to review all sanction updates and report whether they suspect a customer, prospective customer, or transaction (including attempted transactions) is linked to proliferation financing. This will facilitate and ensure timely and effective utilization of the information by the competent authorities.

In their role as gatekeepers, DNFBPs must comply with FTRA 2018 requirements and other relevant AML/CFT/CPF legislation and applicable guidelines. This includes implementing a compliance program that encompasses the obligations listed in the CB's DNFBPs Code of Practice.[44]

Proliferation Financing Vulnerabilities or the DNFBP Sector

DNFBPs can be misused for the purpose of the potential breach, non-implementation or evasion of PF-TFS through the use of trust companies' services providers (accountants and lawyers). A significant PF vulnerability stems from the ease with which these relationships can use opaque corporate entities to engage with the financial system. These networks aim to use opaque corporate entities to conduct seemingly legitimate commercial activity, which is ultimately for the benefit of WMD programs.

Dealers in precious metals and stones (DPMS): Designated persons and entities engaging such dealers to transport gold and diamonds to obtain foreign exchanges to finance their transactions. UNSC 1718 Panel of Experts (PoE) reports highlight an investigation into DPRK diplomatic representatives smuggling gold between two countries in the Middle East (August 2020 Report) and the DPRK's involvement in gold mining in Sub-Saharan Africa (March 2020 Report).

Although the risk of proliferation and proliferation financing in The Bahamas is considered low, product- or service-specific vulnerabilities may include whether a product or service provided by the financial institution or the DNFBP is complex in nature, has a cross-border reach (e.g. via the distribution channels), is easily accessible to customers, attracts a diverse customer base, or is offered by multiple subsidiaries or branches. For a PF risk assessment by a private sector firm, it may consider the vulnerabilities associated with its products, services, customers and transactions. The vulnerabilities refer to weaknesses and features, which could be exploited for sanctions evasion purposes.

[43] For full list, please see https://CB.finance.gov.bs/regulatory-legal-framework/key-legislations/.
[44] See: https://CB.finance.gov.bs/regulatory-legal-framework/codes-of-practice/).

Targeted Financial Sanctions Related to Proliferation

Registrants must ensure facility holder(s) are not from a nation that is subject to sanctions by the UN or similar prohibition from any other official body that would prohibit the establishment of a facility or conduct a transaction.

The CC requests registrants to follow the procedure in section 44 of the Anti-Terrorism Act 2018, including, without delay:

- Freeze all the funds held in the name of a designated entity;
- Inform the Attorney General, the FIU, and CC that a designated entity conducted business with the DNFBP, providing all details of such funds; and
- Inform the designated entity that the funds held at the financial institution have been frozen.

When a DNFBP knows or has reasonable grounds to suspect that any funds maintained on its books are controlled by a sanctioned individual or legal entity but does not report to the FIU i.e., fails to comply with ATA section 44, it commits an offense and is liable on summary conviction to a fine not exceeding $250,000.

Registrants are expected to conduct checks during onboarding of new customers, and apply a risk-based approach to the frequency of sanction screening. The CC assesses compliance with the procedures for UN sanctions through examinations.

Typologies related to PF

Recent typologies identified by the UNSCR 1718 Panel of Experts indicated that designated persons and entities, and those persons and entities acting on their behalf, have quickly adapted to sanctions and developed complex schemes to make it difficult to detect their illicit activities.

According to the US Department of Treasury NRA (February 2022) Proliferation networks work through the interconnected global financial system, seeking methods for appearing to engage in legitimate commercial activity for revenue generation or the procurement of specific goods for their WMD programs. It further states that a key enabler for exploiting this infrastructure is the misuse of legal entities, particularly the ease with which networks can create shell or front companies to obscure who ultimately benefits from the transactions these firms conduct. DNFBPs must take special care with their PF risk assessment to ensure that their vulnerabilities are not being exploited for sanction evasion purposes.

Education and Training

The CC expects that registrants ensure training for all staff is conducted, at least annually, on CPF, including training on The Bahamas' framework for AML/CFT/CPF. These trainings are supplements to the national regulatory framework that must be complied with by all financial institutions.

The CC provides training annually, monthly, and quarterly on AML/CFT/CPF topics, available on its YouTube channel. Additionally, there are training resources on the CB's website for the benefit of registrants.

Self-Risk Assessments

Registrants should conduct a self-risk assessment to understand their firms' ML/TF/PF risk. Policies, procedures, and controls should be guided by the results of the self-risk assessments in an aim to mitigate the risks identified.

6.5 Gaming Board for The Bahamas

The Gaming Board for The Bahamas (GBB) is a statutory authority established in August 1969 in accordance with the Lotteries and Gaming Act 1969. In November 2014, the GBB experienced a significant transformation in the wake of the Government's decision to enact a new suite of legislation to govern gaming operations in The Bahamas, namely:

- The Gaming Act 2014;
- The Gaming Regulations 2014;
- The Gaming House Operator Regulations 2014;
- The Gaming Rules 2015 and;
- The Financial Transaction Reporting (Gaming) Regulations 2014.

The aforementioned legislative frameworks allow the GBB to regulate the domestic gaming sector by providing a broader range of gaming services and products, and establishing an enhanced and robust licensing regime to its licensees, casinos and gaming house operators.

6.5.1 CPF Requirements

Financial Sanctions

Licensees must ensure to implement TFS to comply with UNSC resolutions relating to the prevention, suppression, and disruption of the proliferation of WMDs and its financing. These resolutions require freezing without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UNSC under Chapter VII of the Charter of the United Nations. Licensees are therefore required to:

- Keep abreast of all sanctions notices issued by the UNSC. Licensees are expected to ensure that funds are not made available to entities or individuals seeking to promote the prevention of proliferation financing. In so doing, all licensees shall establish and implement policies and procedures to maintain awareness of the various resolutions adopted by the UNSC.
- Upon receipt of notification of the UNSC Sanctions Listing update, review their database to determine whether the listed entity or individual has any affiliation with the respective casino or gaming house operator.
- Report in writing, findings of the database review to the GBB on or before the date indicated in the notification letter.
- Report in writing, findings during the review, to the FIU and the Office of the Attorney General.

- Immediately freeze the account or any transaction(s) by the patron.[45]
- Maintain the freeze of funds or accounts until further notice by the relevant authorities.

Onboarding Requirements

The GBB requires all licensees to register their potential patrons, conduct KYC measures, and assess any risks that can be associated with their transactions or activities. Patron registration procedure requirements are outlined in Regulation 150 of the Gaming Regulations 2014 and Regulation 19 of the Gaming House Operator Regulations 2014.

Ongoing Requirements

Customer Due Diligence

Upon registration, licensees must execute CDD measures in accordance with the information provided by the patron at registration. Licensees should have appropriate policies and procedures, including stringent CDD rules to promote high ethical and professional standards in the gaming industry to ensure that their establishments are not used, intentionally or unintentionally, for criminal activities before onboarding.

The GBB requires licensees to conduct the following assessments to ensure accurate verification of existing, potential, and new patrons:

- Conduct screening on existing and new patrons.
- Verify all new patrons prior to onboarding to evaluate any risk they may pose to the business. The information shall include but are not limited to the following:
  - Full and correct name of the individual;
  - Address;
  - Date and place of birth; and
  - Purpose of the account and the nature of the business relationship.
- Utilize publicly available reports through the media and the internet, which provides insights into the patron's background.
- Utilize search engines such as World-Check and LexisNexis to gather additional information about the patron.
- Identify the type of business a prospective patron is engaged in to assess whether there is a potential proliferation risk.
- Adopt policies preventing customer relationships with individuals who are from high-risk countries for proliferation financing or countries subject to relevant UN sanctions.
- Have a robust ML/TF/PF risk management program in place that incorporates identifying, monitoring, and reporting suspicious transactions.
- Take appropriate mitigating measures commensurate with the level of risks identified.

[45] Per Section 2 of the Gaming Act 2014, a "patron" means any participant in a gaming activity, other than the holder of a license issued under the Act.

Enhanced Due Diligence

GBB requires its licensees to apply EDD measures in addition to the aforementioned requirements to manage and mitigate the proliferation financing risks arising in the following cases:

- The gaming licensee has determined that a patron or potential patron is a PEP or a family member or known close associate of a PEP.
- Where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction(s) have no apparent economic or legal purpose.

Depending on the circumstance, licensees should conduct EDD measures, which may include, but are not limited to:

- Source of wealth verification;
- Verification of patron information through searches of additional independent and trusted sources;
- Additional measures to better understand the context, ownership, and financial background of the patron; and
- Enhanced monitoring to ensure that patron transactions coincides with the patron's profile.

When conducting business with customers that reside in high-risk countries or when conducting transactions in which one of the parties to the transaction resides in a high-risk country, licensees must conduct the following enhanced measures:

- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds and source of wealth of the potential patron;
- Obtaining information on the type of transactions;
- Obtaining approval of senior management to establish or continue the business relationship; and
- Enhance monitoring of business relationships by increasing the number and timing of controls applied and selecting patterns of transactions that require further review.

Red Flag Indicators

Licensees are to be aware of the potential proliferation financing, red flag indicators as provided below:

- The patron has ties to a foreign country of proliferation concern, or a neighbouring sympathetic country.
- Patron is involved in the supply, sale, delivery, or purchase of dual-use, proliferation-sensitive or military goods, particularly to higher-risk jurisdictions.
- Patron's address or telephone number is the same or similar to an individual found on sanctions lists.
- The potential patron or supplier is connected with a higher-risk jurisdiction of proliferation concern.
- The patron activity does not match the patron's profile.
- The patron provides incomplete information, or is resistant to providing additional information when sought.

- Patron purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino cheque.
- Patron puts money into slot machine and claims accumulated credits as a jackpot win.
- Patron exchanges small denomination bank notes for large denomination bank notes, chip purchases vouchers or cheques.

Risk-Based Approach

Licensees' Risk-Based Approach shall incorporate controls to mitigate the risk of proliferation financing within their current AML/CFT structure. As such, Gaming Licensees shall implement policies, which prevent the formation of patron relationships that expose their operations to countries that are at higher risk for proliferation financing.

Through the adoption of a risk-based approach, Gaming Licensees can assess whether their patron or potential patron is from a jurisdiction that is subject to any UN sanctions; and also exercise ongoing due diligence. Essentially, the GBB expects the gaming licensee to use reasonable efforts to create and maintain supporting records and have clear policies, procedures, and controls relative to maintaining records, which facilitates proper evaluate of the PF risks at Casinos or Gaming Houses.

Training

Licensees should provide training to their staff at least annually in relation to PF matters. Records are to be retained of all training undertaken by staff of the Casino and Gaming Houses. Training provided to staff of Casinos and Gaming House Operators relative to PF may include:

- Trends, typologies, and PF patterns;
- Any other workshops, conferences, seminars, or the like, which will increase awareness on the prevention and suppression of proliferation and proliferation financing; and
- The AML/CFT/CPF legislative framework.

7 Conclusion

Preventing proliferation and its financing remains an area of high importance for the GFSR. The FATF has provided updated guidance to assist jurisdictions with combating AML/CFT/CPF in the face of new financial products and technologies, reinforcing the principle that jurisdictions and their constituent entities must continually review their AML/CFT/CPF strategies to ensure that they remain effective as individuals continue to innovate. While the threat of PF is low in The Bahamas, ensuring it remains low will require cooperation on both a national and international scale. Identifying, assessing, and understanding proliferation financing risks will assist the country and its entities in preventing designated persons involved in PF from raising and using funds.

The GFSR provides these CPF Guidelines as supplementary material to the aforementioned CPF legislative framework and is intended to act as a reminder of and explanation for the duties and obligations of registrants and licensees of GFSR members.

Contact Information

Central Bank of The Bahamas
Tel: 1 (242) 302-2600
Email: cbob@centralbankbahamas.com
Website: centralbankbahamas.com

Securities Commission of The Bahamas
Tel: 1 (242) 397-4100
Email: info@scb.gov.bs
Website: scb.gov.bs

Insurance Commission of The Bahamas
Tel: 1 (242) 397-4183 / 376-7242
Email: info@icb.gov.bs
Website: insurancecommissionbahamas.com

Compliance Commission of The Bahamas
Tel: 1 (242) 604-4331
Email: compliance@bahamas.gov.bs
Website: CB.finance.gov.bs

Gaming Board for The Bahamas
Tel: 1 (242) 397-9200
Email: info@bahamasgamingboard.com
Website: gamingboardbahamas.com

Financial Intelligence Unit
Tel: 1 (242) 397-6300
Email: director.fiu@fiubahamas.bs
Website: fiubahamas.org.bs

Countering Proliferation Financing Guidelines

Group of Financial Services Regulators:
Central Bank of The Bahamas
Securities Commission of The Bahamas
Insurance Commission of The Bahamas
Compliance Commission of The Bahamas
Gaming Board for The Bahamas