GUIDANCE NOTE ON CONDUCTING AN INSTITUTIONAL PROLIFERATION FINANCING RISK ASSESSMENT 2025

NBFIRA

Non-Bank Financial Institutions Regulatory Authority

Contents

1. PURPOSE

This guidance is issued by the Non-Bank Financial Institutions Regulatory Authority (NBFIRA) in accordance with section 49(1)(c) of the Financial Intelligence Act that provides that, through consultation with the Financial Intelligence Agency (FIA) supervisory authorities shall establish and issue guidance notes and provide feedback to help a specified party comply with the Act. This guidance note is issued to provide guidance on how to conduct an institutional proliferation financing risk assessment.

2. SCOPE

This Guidance Note applies to institutions licenced, exempted and supervised by Non-Bank Financial Institutions Regulatory Authority (the Authority) through various primary and secondary legislation (i.e., NBFIs). It specifies considerations for AML/CFT/CPF programme of a regulated entity. The guidelines are not intended to be exhaustive nor to set limits on steps to be taken by regulated entities to detect, prevent and report financial crimes.

3. ASSOCIATED DOCUMENTS

Document	Reference
Financial Intelligence Act, 2022	Cap 08:07
Financial Intelligence (Implementation of United Nations Security Council Resolutions) Regulations	Statutory Instrument No. 13 of 2022
Financial Action Task Force (FATF) Recommendations	Amended June 2025
Chemical Weapons (Prohibition) Act	Cap:24:04
Biological Weapons (Prohibition) Act	Cap. 24:06
Nuclear Weapons (Prohibition) Act	Cap 24:05
Counter Terrorism Act	Cap 08:08 of 2014
Chemical, Biological, Nuclear and Radiological Weapons Management Authority, established under the Chemical Weapons Prohibition Act	Cap:24:04
Royal United Services Institute (RUSI) Institutional Proliferation Finance Risk Assessment Guide	June 2023

4. DEFINITIONS

Term	Definition
Dual-use goods	Goods, software and/or technologies that can be used for both commercial and military purposes. Such goods include nuclear materials, electronics, computers, sensors and lasers, etc.
Proliferation of Weapons of Mass Destruction	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.
Weapons of Mass Destruction	Weapons that can cause widespread death and destruction, affect large numbers of people and cause significant damage to infrastructure and the environment. These weapons typically include nuclear, chemical, and biological weapons, but can also encompass other devices with similar destructive potential.

5. ACRONYMS AND ABBREVIATIONS

Abbreviation	
CDD	Customer Due Diligence
FATF	Financial Action Task Force
FI Act	Financial Intelligence Act
FI	Financial Institution/s
KYC	Know-Your-Customer
ML	Money Laundering
NRA	National Risk Assessment
PIP	Prominent and Influential Person
PF	Proliferation Financing
TF	Terrorism Financing
UNPoE	United Nations Panel of Experts
UNSC	United Nations Security Council
WMD	Weapons of Mass Destruction

6. RESPONSIBILITIES

Boards of directors or the most senior management, where a board of directors is not present, of NBFIs are accountable and responsible for their entity's compliance with the provisions of the FI Act and all other financial services laws. The responsibility may be delegated to management to ensure compliance during day-to-day business activities as conducted by NBFI.

7. UNDERSTANDING PROLIFERATION FINANCING RISK

Proliferation financing is the financial backbone supporting the development and distribution of WMDs. The global community combats proliferation financing through United Nations Security Council resolutions (UNSCRs), FATF recommendations and efforts of governments, and regulatory bodies and the private sector. The FATF requires countries to implement targeted financial sanctions without delay to comply with UNSCRs, adopted under Chapter VII of the Charter of the UN concerning the prevention, suppression and disruption of proliferation of WMD. UNSCRs require countries to freeze 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 United Nations Security Council (UNSC) under Chapter VII of the Charter of the United Nations. To prevent such activities, several UNSCRs impose international legal obligations related to proliferation financing:

(a) UN Security Council Resolution 1540, adopted in 2004, addresses the proliferation of weapons of mass destruction (WMDs) by obligating all states to take measures to prevent non-state actors from manufacturing, acquiring, possessing, developing, transporting, transferring or using such weapons and related materials

(b) United Nations Security Council Resolution 2231, adopted in 2015, endorsing the Joint Comprehensive Plan of Action on the nuclear program of Iran. It sets out an inspection process and schedule while also preparing for the removal of United Nations sanctions against Iran. However, the conventional arms embargo and travel bans ended in October 2020 and the restrictions on transferring missiles and drones ended in October 2023.

Further, FATF standards establish international rules for the implementation of targeted financial sanctions relating to the prevention, suppression and disruption

of proliferation of WMD and its financing. FATF has issued the below recommendations relating to proliferation financing.

(a) Recommendation 7, which requires countries to freeze, 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 UN.
(b) Recommendation 2, which calls on cooperation and coordination of the relevant authorities to combat Money laundering, Terrorist financing and PF.
(c) Recommendation 1, which requires countries, financial institutions, designated non-financial businesses and professionals, virtual asset service providers, and non-profit organisations to identify and assess the risks of potential breaches, non-implementation or evasion of TFS-PF and to take action to mitigate them.
(d) Recommendation 15, which requires countries to identify and assess their PF risk and establish mitigation measures in respect of virtual assets.

NBFIs are also required to undertake PF risk assessments at institutional level to identify, assess and take effective action to mitigate their money laundering, terrorist financing and proliferation financing risks.

There are three key stages in proliferation financing;

(a) Fundraising: the proliferator sources funds from state budgets, or from illegitimate or legitimate commercial or criminal activities conducted overseas by or on behalf of state actors.
(b) Disguising and placing funds into the financial system: proliferators rely on a network of businesses, front companies, opaque ownership structures and brokers to ensure that everything appears geographically separate from sanctioned countries.
(c) Procuring materials and technology using those funds: the proliferator accesses the international financial system to pay for goods, materials, technology and logistics needed for its WMD programme.

7.1 DIFFERENCES AND SIMILARITIES BETWEEN PF, ML AND TF

Table 1: PF, ML and TF: A Comparison

	Proliferation Finance	**Money Laundering**	**Terrorism Financing**
Purpose	To support states and non-state actors in their illicit development of WMD programmes.	To launder proceeds of crime to make them look legitimate.	To finance terrorism, terrorists, and terrorist organisations.
Use of formal financial systems?	Yes, as well as cross-border smuggling of cash, gold or other high-value goods by 'mules' to support state and non-state proliferation activities.	Yes, as well as informal financial conduits such as hawala, currency exchange houses, cash couriers and smuggling.	Yes, as well as informal financial conduits such as hawala, currency exchange houses, cash couriers and smuggling.
Transactions	Transactions appear legitimate and aligned to traditional commercial activity, structured as in ML to hide the connection with state and non-state actors involved in proliferation financing, or to hide the end use or the end user of dual-use goods purchased.	Complex web of transactions, involving the use of funds, real estate, shell or front companies, offshore centres, tax havens, and complex layers of legal entities (including trusts and foundations, for example).	Multiple methods, including the use of traditional payment methods and banking activities, informal value transfer systems, cash and precious metals and stones smuggling.
Size of transactions	Medium	Small to large	Small to medium

Activities and sectors	-Complex structuring to hide the origin of the funding as well as what funds/assets are ultimately intended to be used for. -Exposure to all sectors. For example, purchase of dual-use items such as engine parts, raising of funds through network of overseas works, exploitation of construction companies or fisheries.	-Complex structuring and web of transactions that may involve using front companies, e.g. cash-intensive businesses (such as restaurants, convenience stores and nail bars) -Exposure to all sectors. For example, purchase of luxury items with tainted/criminally obtained funds.	-Multiple, varied methods, for example, formal banking systems, smuggling of valuables (precious metals and stones, antiquities) and cash. -Exposure to all sectors, e.g., procurement of weapons and vehicles
Money trail	Linear: movement of finances and/or trade in proliferation-sensitive goods to state and non-state actors.	Circular: the funds tend to eventually end up back with the person who generated them once the funds have been sufficiently distanced from the crime.	Linear: funds are used to promote and finance terrorists and their activities, as well as in their risk assessment structure, by raising, storing, moving and using funds.

7.2 PROLIFERATION FINANCING RISK ASSESSMENT METHODOLOGY

An institutional proliferation financing risk assessment can be defined as a process of identification, assessment and understanding of proliferation financing risks at institutional level to determine the risk levels of financial crime on their operations and related party activities, the threats and vulnerabilities.

These risks may be categorised as follows:

(a) Customers
(b) Products and services offered
(c) Jurisdictions operated in and with
(d) Transactions
(e) Delivery channels used

Each of these risk categories will be risk-assessed by reviewing their underlying risk factors and evaluating the proliferation financing residual risk they represent.

7.2.1 INHERENT RISKS

Inherent risks are the proliferation financing risks an institution faces before taking into account the controls and mitigation strategies that have been applied. Once risk categories have been identified, NBFIs should assess the inherent risk of these categories by considering the likelihood of the risk materialising, alongside the impact of the event should it materialise.

7.2.2 IDENTIFYING CONTROLS AND ASSESSING THE EFFECTIVENESS OF CONTROLS

Once the inherent risk has been evaluated, the next step is to assess the institution's residual proliferation financing risks, i.e., risks that remain after controls and mitigation strategies to tackle inherent risks have been applied. Further to obtaining and maintaining customer information at onboarding and as part of the ongoing business relationship, NBFIs should also establish;

(a) Significant controllers, intermediary entities within an ownership chain, and signatories (to establish whether there are any links to a sanctioned party or sanctioned jurisdiction).
(b) Whether the customer deals in dual-use goods or research, or military goods.
(c) The expected activity on the account.

In addition, understanding whether the customer is purchasing, selling, importing or exporting dual-use or other controlled goods is essential to proliferation financing. More specifically, institutions need to know:

(a) Whether the customer is licensed to trade in such goods.
(b) Whether there is a link to a sanctioned jurisdiction or to an area that borders a sanctioned jurisdiction.
(c) Whether trades involve the transshipment of goods.

Similarly, NBFIs should screen new and existing customers (as well as related parties and/or counterparties) against sanctions lists, adverse media and watchlists to identify any links to sanctioned entities or nationals, or Prominent Influential Persons (PIPs). Any alerts and true matches should be managed as per the NBFI's existing escalation processes. Customers (and relevant related parties) should be subject to ongoing screening throughout their relationship or the lifecycle of the trade.

Furthermore, NBFIs' transaction monitoring tools should include typologies indicative of proliferation financing activities. Where such transactions are identified, an investigation must be undertaken as per the FI's existing processes to identify sanctions evasion and/or proliferation financing. Any suspicion arising will need to be reported to relevant sanctions authorities as well as to the Financial Intelligence Agency.

Finally, all members of staff should complete relevant training appropriate to their role. More specifically, staff who perform customer onboarding, risk assessments, ongoing monitoring, or name and transaction screening should be given targeted training on proliferation financing risks, typologies and risk indicators.

In summary, existing controls that support NBFIs in mitigating proliferation financing risks include:

(a) Governance structures.
(b) Counter proliferation financing policies.
(c) Implementation of recommendations based on findings from PF risk assessments (National/Sectoral/Intuitional)
(d) CDD/ KYC arrangements (including ongoing due diligence and enhanced due diligence).
(e) Know Your Employee checks.
(f) PIP, sanctions and watchlist screening.
(g) Ability to freeze assets of designated entities and/or individuals.
(h) Transaction monitoring.
(i) Independent controls testing and quality assurance of existing systems and controls.
(j) New product approval processes, including, where applicable, committee decisions.
(k) Staff training.
(l) Restrictions on operating in certain markets
(m) Suspicious activity reporting.
(n) Business-wide risk assessments.

The above list is not exhaustive, and there are additional elements that should be introduced to specifically target proliferation financing. These are:

(a) Calibrating transaction monitoring tools to reflect existing proliferation financing scenarios.

(b) Reviewing United Nations Panel of Experts (UNPoE) reports for North Korea and Iran to identify natural persons and entities associated with proliferation financing and adding these to internal watchlists.

(c) Reviewing UNPoE reports for North Korea and Iran to identify emerging proliferation financing typologies and trends.
(d) Providing export/import controls training to employees.
(e) Providing dual-use goods training to employees.

The effectiveness of controls is determined by two considerations: whether the control is well designed to mitigate inherent risks, and whether the control is being adequately operated to mitigate those risks. The combined design effectiveness and operating effectiveness of a control indicates whether the control is ineffective, partially effective, effective or highly effective. The determination as to whether controls are designed and operated effectively should be based on control testing.

7.2.3 VULNERABILITY TO PROLIFERATION FINANCING RISK

Once institutions have completed their proliferation financing risk assessments, they can measure their residual risk, and hence their vulnerability to proliferation financing risk. Institutions can subsequently choose whether to accept, further mitigate or prevent such vulnerabilities and exposures to proliferation financing risk. Operating under a risk-based approach, institutions should aim to target the highest-rated identified inherent risks. In this spirit, institutions may also decide to review certain controls that may be seen as disproportionate in terms of mitigating lower inherent risks.

7.3 PROLIFERATION FINANCING RISK CATEGORIES AND RISK FACTORS

NBFIs will then need to consider each risk against the risk factors relevant to their business activities. The prominence of specific risk factors will vary across institutions. For example, a small insurance company would not have the same business exposure as an international FI, or a virtual asset service provider. Risk factors will vary depending on the type of markets the institution services, its customers, the products it offers, delivery channels and platforms used.

Risk Categories	Risk Factors	Potential Acts of Proliferation Finance
Customer risk (including legal entity type)	-Residency and nationality -Complex ownership structure involving several jurisdiction and entity types -Use of international corporate vehicles -Virtual currency providers or customers investing via such providers -Companies with nominee shareholders	-Use of a country's vulnerability to proliferation financing because of historical legacy, poor regulatory and legal framework, social and political factors, or economic and technological factors. -Jurisdictions providing accounts to, or otherwise facilitating, financial activities of proliferation states. -Use of local branches of banks and financial institutions based in countries of proliferation concern. -Use of complex structures (such as multi-layered trusts, foundations), nominee directors and/or shareholders to hide a UBO or significant controller and their association with sanctioned entities or jurisdictions. -Use of cryptocurrencies to avoid the formal financial system. -Establishment of corporate networks that facilitate but may not be solely involved in proliferation financing activities. Ultimate beneficial ownership, connections and control structures are opaque. -Use of front companies, shell companies or brokers to obtain trade finance products and services, or as parties to clean payments.
Business activity/ occupation/ industry of customer	-Money services businesses -Suppliers, buyers and trading partners in WMD technology/dual-use goods/nuclear/defence industries -Maritime/shipping industry -Money-exchange businesses -Embassies and consulates -PIPs -Corporate service providers and intermediaries	-Use of universities or research centers to procure dual-use goods and/or for payment of funds -Use of shipping companies, brokers and agents to obtain insurance or other financial services related to maritime transport. Often combined with use of front companies with opaque ownership structures. -Money-exchange businesses used for cash transfers in support of proliferation networks, where transfers involve individuals or entities owned or controlled by proliferation actors. It can also involve structured payments to organised crime networks involved in revenue-raising activities. -Use of diplomats, consular officers or diplomatic or consular missions of North Korea to build networks, including corporate networks, within a country. These networks then facilitate a range of revenue-raising activities as well as facilitating financial products or services related to trade in goods. -Use of PEPs who are vulnerable to corruption and may leverage their position of power to access land rights, mining rights or exploit businesses (such as

		fisheries) to raise revenue for sanctioned countries and actors. -Use of professional intermediaries and corporate service providers to mask parties to transactions and end users associated with proliferation financing.
Geographic risk	-Jurisdictions known for diversion -High-risk jurisdictions and high-risk third countries -Countries subject to sanctions or embargos; countries identified as lacking appropriate AML/ CFT laws and regulations -Offshore financial centers and non-cooperative tax jurisdictions -Jurisdictions identified as having significant levels of corruption or organised crime, or other criminal activity -Jurisdictions identified as providing funding or support to terrorist activities	-Use of local branches of banks and financial institutions based in countries of proliferation concern. -Use of third countries with weak counter proliferation financing frameworks or elevated risks of corruption and bribery to channel financial transactions related to dual-use goods. -Use of offshore jurisdictions that offer the possibility of easily creating front and/or shell companies to disguise UBOs and/ or end users associated with WMD programmes. -Use of trade or other economic relations with countries with links or significant exposure to a proliferating country. Often facilitated by a complex corporate network.
Products, services and transactions risk	-Open account payments/ letters of credit -International payments -Foreign accounts -Provision of precious metals and stones services -Provision of maritime insurance products -Provision of virtual assets trading	-Use of trade finance products and services and clean payment services in procurement of proliferation-sensitive goods. -Use of fake or fraudulent documents related to shipping, customs or payments to facilitate transactions or trade finance. -Use of foreign-denominated accounts to make international payments for dual-use goods, or to transfer proceeds of revenue-raising activities. -Purchase or sale of precious metals and/or stones to transfer value across jurisdictions or to raise revenue to support WMD programmes.

		-Provision of maritime insurance to shipping companies involved in sanctions violations. -Use of cryptocurrencies to leverage anonymity and avoid the formal financial system and associated controls that may more easily identify sanctions violation.
Delivery channel risk	-Face-to-face origination -Non-face-to-face origination	-Use of non-face-to-face account opening facilities to mask the identity of the UBO. -Services that can conceal beneficial ownership from competent authorities (for example, nominee director risk).

COUNTRY RISK SCORING

Country risks refers to the heightened threats posed by countries with insufficient controls to prevent their financial systems from being used to finance the development of WMD. Key risks include the ease with which such countries facilitate the movement of proliferation-sensitive items and their potential to exploit financial loopholes, making them high-risk jurisdictions for international financial activity.

Scoring	**Description**
Restricted	-Country is subject to UN sanctions (North Korea)-Country is subject to other sanctions (for example, China, Russia and Pakistan). Country has significant corporate/trade network of proliferation financing state/ties with sanctioned country/ countries. -Country offers shipping flags of convenience or passports of convenience. -Intelligence suggests that country may consider developing nuclear capability through illicit procurement.
Medium–High	-Known country of diversion, country scored with a low level of effectiveness in mutual evaluation reports, including on Immediate Outcome 11.27 -Geographical proximity to a proliferating country. -Country named by the UNPoE/Office of Foreign Assets Control/mainstream media as either trading with

	sanctioned states or lacking sufficient visibility/transparency on trade patterns. -Country outside the Nuclear Non-Proliferation Treaty and/or country is maintaining or improving, or is expected to maintain or improve, its nuclear capabilities. - Proliferating state has diplomatic presence in the country.
Medium–Low	-Country neighbours a proliferating state. -Country has a large diaspora from a state of proliferation concern. -Country hosts a financial, trade centre, or transhipment hub that is attractive to proliferation financiers. -The jurisdiction is home to a manufacturing sector that produces goods controlled by international supplier regimes related to WMD and/or their delivery vehicles. -The jurisdiction has weak controls and/or enforcements in relation to ML, TF and proliferation financing.

NB: This guidance is adopted from the Royal United Services Institute (RUSI): Institutional Proliferation Finance Risk Assessment Guide, published in June, 2023. The document can be accessed at www.rusi.org.