PAPUA NEW GUINEA

SANCTIONS SECRETARIAT

(In collaboration with the Financial Analysis and Supervision Unit and Department of Justice & Attorney-General)

GUIDELINES FOR FINANCIAL INSTITUTIONS

ON THE IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS UNDER THE UNITED NATIONS FINANCIAL SANCTIONS ACT 2015

(Disclaimer: This guide summarises publicly available information from the UN sanctions committees and the PNG Sanctions Secretariat. It is not legal advice.)

Table of Contents

I. INTRODUCTION

1.1 PURPOSE AND OBJECTIVE

These guidelines have been developed by the Sanctions Secretariat of Papua New Guinea in collaboration with the Financial Analysis and Supervision Unit (FASU) and Department of Justice & Attorney-General (DJAG) and with assistance from the Asian Development Bank (ADB) as a reference source to assist financial institutions (FIs) in complying with the requirements of the United Nations Financial Sanctions Act 2015 (UNFSA). The purpose is to protect the public, and the financial system of Papua New Guinea, by helping to ensure that FIs are not utilized, whether purposely or unwittingly, for terrorist financing (TF) or financing of weapons of mass destruction (WMDs), referred to here as "proliferation financing" (PF).

1.2 WHY ARE FINANCIAL SANCTIONS NECESSARY IN PNG?

Terrorist Financing

Although currently TF risk in PNG is considered to be low, this situation could change rapidly. Unless the issue is kept under very active review, there is a real danger that PNG could become a conduit to channel or store funds that could be used for carrying out terrorist acts. Given the very small amounts of money needed to fund terrorist activity, these may well escape detection. The emerging informal value transfer operations in PNG also provide a significant risk that need to be better understood and scrutinised by the FASU, the Royal Papua New Guinea Constabulary (RPNGC) and the banks which might be used to move larger amounts to offset transactions.[1] There is therefore good reason for FIs to be diligent in instituting measures to counteract these undesirable circumstances.

Proliferation Financing

Similarly, PNG's current exposure to WMD-related sanctions evasion of PF is relatively moderate.[2] However, there is good reason for FIs to be diligent in their efforts to combat PF, just as with TF. While WMDs may be quite sophisticated (such as a long-range missile system), they can also be as simple as a crude home-made explosive device. Detection and prevention of PF can be particularly difficult because the materials, parts, equipment, technology, or expertise used in WMD production may also have legitimate uses.

1.3 WHAT ARE FINANCIAL SANCTIONS?

Under sections 14 and 15 of the UNFSA, sanctions are prohibitions on:

- dealing with assets belonging to or owned, held or controlled (directly or indirectly) by a "designated person or entity" (DPE) ("asset freezes"); and

- making assets or financial services available directly or indirectly to, or for the benefit of, a DPE.

[1] National Risk Assessment, pp. 22-25, 131.
[2] 2024 MER, p. 9, par. 23 and Chapter 4, *Terrorist Financing and Financing of Proliferation,* Key Findings, Section 10.11, p. 77.

These sections of the UNFSA implement specific resolutions of the United Nations Security Council (UNSC)[3] and Recommendations 6 and 7 of the Financial Action Task Force (FATF), which are aimed at countering TF and PF.

Links to the UNSC sanctions lists, as well as the "Consolidated List" maintained by the PNG Sanctions Secretariat, are provided below:

List	Direct link
DPRK (1718 Committee) Sanctions List	https://main.un.org/securitycouncil/en/sanctions/1718/materials main.un.org
ISIL (Da'esh) & Al-Qaida (1267/1989 Committee) Sanctions List	https://main.un.org/securitycouncil/en/sanctions/1267 main.un.org
Taliban (1988 Committee) Sanctions List	https://main.un.org/securitycouncil/en/sanctions/1988 main.un.org
Iran – Annex B to UNSCR 2231	https://main.un.org/securitycouncil/en/content/2231/list main.un.org
PNG Consolidated List & local guidance	https://pngsanctionssecretariat.gov.pg/ (see "Consolidated List" tab) pngsanctionssecretariat.gov.pg

1.4 Overview of the Legislative Framework For Sanctions in PNG

The legislative framework regarding financial sanctions in PNG consists of:

- the Criminal Code Act 1974 (Criminal Code Act), as amended by the Criminal Code (Money Laundering and Terrorist Financing) (Amendment) Act 2015 (the Criminal Code Amendment Act);
- the UNFSA; and
- the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (AML/CTF Act).

The Criminal Code Act

The Criminal Code Amendment Act introduced comprehensive and effective criminal law provisions to create a comprehensive offence for TF in the Criminal Code Act 1974. Per the 2015 amendments, Section 508J of the Criminal Code Act ("Terrorist Financing") makes it a crime for a person, by any means, to directly or indirectly provide or collect property with the intention or knowledge that it be used to finance a terrorist act, a terrorist (without lawful justification) or a terrorist organisation. Such action is an offence under Section 508J:

[3] These UNSC Resolutions are listed in Schedules 1 and 2 of the UNFSA. Schedule 1 includes: Resolutions on Al-Qaida (Resolutions 1267/1989 and successor resolutions); Resolutions on the Taliban (Resolution 1988 and successor resolutions); Resolutions on Democratic People's Republic of Korea (DPRK) (Resolution 1718 and successor resolutions); and Resolutions on Iran (Resolution 1737 and successor resolutions). Schedule 2 refers to Resolution 1373 on the suppression of terrorism and successor resolutions.

- even if a terrorist act does not occur or is not attempted;
- even if the property was not actually used to commit or attempt to commit a terrorist act, or linked to a specific terrorist act;
- regardless of whether the property was from a legitimate or illegitimate source;
- regardless of the country in which the terrorist or terrorist organization is located; and
- regardless of the country in which the terrorist act has occurred or is intended to occur.

"Property" is broadly defined. Per Section 508I of the Criminal Code Act, property means:

> "assets of every kind, whether tangible or intangible, corporeal or incorporeal, moveable or immovable, however acquired, including an enforceable right of action, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including but not limited to currency, bank credits, deposits and other financial resources, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, whether situated in Papua New Guinea or elsewhere, and includes a legal or equitable interest, whether full or partial, in any such assets."

Section 508I of the Criminal Code Act provides for the definition of key aspects of TF such as "terrorist," "terrorist act," and "terrorist organisation." These key definitions are also applied in the UNFSA specifically for the designation process described below. Per Section 508I of the Criminal Code Act, a "terrorist" means any natural person who:

- commits, enables, aids, counsels or procures a terrorist act;
- attempts to commit a terrorist act; or
- conspires to commit (whether directly or indirectly) a terrorist act.

A "terrorist organization" means a group of persons or a body corporate that:

- commits, enables, aids, counsels or procures a terrorist act;
- attempts to commit a terrorist act; or
- conspires to commit (whether directly or indirectly) a terrorist act.

Per Section 508I of the Criminal Code Act, there are two types of terrorist acts:

- an act which is an offence under any of the following treaties:
  - the Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970;
  - the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971;
  - the Convention on the Prevention and Punishment of Crimes against

Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973;
  - the International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979;
  - the Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980; and
  - the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988;
  - the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988;
  - the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988;
  - the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997;

- any other act or threat of action that:
  - involves serious violence against a person not taking an active part in hostilities in a situation of armed conflict;
  - involves serious damage to property;
  - endangers another person's life;
  - creates a serious risk to the health or safety of the public or a section of the public; or
  - is designed to seriously interfere with or to seriously disrupt an electronic system;

  and
  - is designed to influence a government, or international organisation or to intimidate the public or a section of the public; or
  - is made for the purpose of advancing a political, religious or ideological cause.

The UNFSA

Section 14 of the UNFSA prohibits FIs from:

- dealing with an asset knowing that the asset is owned, controlled or held, directly or indirectly, wholly or jointly, by or on behalf of or at the direction of a DPE;

- dealing with an asset reckless as to whether the asset is owned, controlled or held, directly or indirectly, wholly or jointly, by or on behalf of or at the direction of a DPE.

Section 15 of the UNFSA prohibits FIs from:

- making an asset or financial service available knowing that it is being made available, directly or indirectly, wholly or jointly, to a DPE or a person or entity owned or controlled by, or acting on behalf of, a DPE;

- making an asset or financial service available to any person knowing that the asset or financial service is for the benefit of a DPE;

- making an asset or financial service available reckless as to whether it is being made available, directly or indirectly, wholly or jointly, to a DPE or a person or entity owned or controlled, or acting on behalf of a DPE; or

- making an asset or financial service available to any person reckless as to whether the asset or financial service is for the benefit of a DPE.

The AML/CFT Act

Under section 40 of the AML/CTF Act, an FI must report to FASU any assets which it holds of a DPE. The report must be made as soon as is reasonably practicable or within 10 working days from the date notification of a designation is received.

Part 2 below explains the sanctions process under the UNFSA and AML/CFT Act in more detail.

1.5 WHY IS A FINANCIAL SANCTIONS REGIME IMPORTANT FOR PNG?

A key feature of TF and PF is that they have no boundaries. Terrorists and WMD financiers are always looking for gaps across jurisdictions to find safe havens for illicit assets. It is important for PNG, and other countries in the region, to ensure that their laws are robust and comprehensive, to close any potential gaps that terrorists and financiers of WMDs can exploit.

1.6 CHALLENGES FOR FIS: UNDERSTANDING SANCTIONS EVASION

DPEs will rarely – if ever – show up in a transaction but will instead utilize well-rehearsed tricks to conceal who they are and where the money or goods are going. It is therefore crucial that FIs consider how DPEs may indirectly attempt to gain access to funds or financial services. Common sanctions evasion techniques used by DPEs include:

Evasion tactic	What it looks like in real life
1. Fake or "front" companies	A new firm with no track record, often registered overseas, suddenly orders high-value goods or opens accounts.
2. "Straw" customers or clients	A person who purports to be acting on his/her own behalf, but is in fact acting on behalf of an undisclosed DPE. Such customers may be unfamiliar with the business they claim to represent, or with the transaction they are undertaking.
3. Non-transparent ownership structures	A company that is part of a corporate group whose ownership or control structure is extremely convoluted or confusing for no apparent business or economic reason.
4. False information	The use of aliases and/or falsified documentation to hide involvement of a DPE.
5. Doing business in high-risk jurisdictions	Customers/clients who are located or do significant business in high-risk jurisdictions (i.e., jurisdictions known to be locations for terrorist activity, public corruption, or financial crime).
6. Suspicious shipping moves	Ships that switch off their trackers, change names or flags mid-voyage, or transfer cargo at sea so paperwork shows the wrong port or owner.

Evasion tactic	What it looks like in real life
7. Mislabelled trade paperwork	Invoices that under-price, use incorrect HS codes, or claim the buyer is in a low-risk country, even though the goods ultimately end up in the DPRK or Iran.
8. Money moved in small pieces	Dozens of low-value transfers through different banks or money-transfer agents ("smurfs") to keep each payment below monitoring thresholds.
9. Cryptocurrency detours	Funds converted to Bitcoin or privacy coins, sent through mixing services, then cashed out on an exchange with weak controls.
10. "Charity" or NGO cover	A non-profit organisation raises donations supposedly for "humanitarian aid" but quietly sends the cash or dual-use items to a sanctioned group.
11. Help from professional enablers	Lawyers, accountants or company-service providers who set up the structures, open accounts, or re-flag ships for a hidden client.

2. OPERATION OF THE PNG FINANCIAL SANCTIONS REGIME

2.1 THE SANCTIONS SECRETARIAT

Section 25 of the UNFSA establishes the Sanctions Secretariat within the Department of Prime Minister and National Executive Council. As the secretariat to the National Security Advisory Committee, the Sanctions Secretariat has an integral role in the effective implementation of a successful financial sanctions regime in PNG. It performs a number of key functions, including:

- providing support to the National Security Advisory Committee and the Prime Minister in exercising designation powers;
- maintaining an up-to-date Consolidated List of DPEs, which consists of four UNSC Committee Sanctions Lists implementing the UNSC Resolutions listed in note 1 above on Al-Qaida, the Taliban, the DPRK and Iran;
- issuing public guidance to promote and assist compliance with PNG's financial sanctions legislation.

Other functions include:

- receiving proposed designations from agencies within PNG and from foreign agencies (including preparing internal recommendations for such designations);
- notifying FIs and DNFBPs (and others) of designations through the FASU;
- preparing guidelines and forms for use by FIs, DNFBPs and the public;
- receiving and responding to enquiries from the public and private sector about authorisations to deal with frozen asset of designated entities; and

- generally raising awareness about the risks and dangers of money laundering and terrorist financing.

The Sanctions Secretariat's website contains valuable information for FIs, including identification of DPEs and regular updates. The website is located at https://pngsanctionssecretariat.gov.pg.

2.2 DESIGNATED PERSON OR ENTITY STATUS

According to Section 5 of the UNFSA, a "designated person or entity" means a person or entity –

(a) designated by the Prime Minister or the court under the UNFSA; or

(b) designated by the United Nations Security Council or its Committees pursuant to Resolutions listed in Schedule 1 to the UNFSA or prescribed by Regulations made under Subsection 29(2) of the UNFSA.

The Prime Minister, through the Sanctions Secretariat and FASU, notifies FIs and DNFBPs of a designation, redesignation, revocation and expiry. The notifications are also published in the National Gazette. Publication in the National Gazette is not required where the United Nations Security Council (UNSC) or its Committees make a designation or revocation in respect of a person located outside PNG.

The UNSC has made all DPEs to date. There have been no domestic designations, and all UNSC-designated DPEs are located outside of PNG.

The UNSC DPEs have immediate application in PNG and the immediate effect of imposing the prohibitions in the UNFSA. Upon a UNSC designation or redesignation, FIs and DNFBPs must immediately cease dealing with an asset and cease to make available financial services where:

- the asset is held directly or indirectly, wholly or jointly by or on behalf of or at the direction of a DPE;

- the asset or financial service is made available directly or indirectly, wholly or jointly to a DPE or a person or entity owned or controlled or acting on behalf of a DPE; or

- the asset or financial service is for the benefit of a DPE.

Likewise, if a person's DPE status has been revoked, the prohibitions in the UNFSA cease to apply.

The above situation could change in the future, and FIs should therefore keep informed as to any domestic designations that may be implemented under the UNFSA.

The current number of DPEs on each UN sanctions list is provided below:

Sanctions group	Individuals	Entities/undertakings	Total	Source & last update (June 2025)
DPRK (1718 Committee)	**80**	**75**	**155**	**UN 1718 list page, updated 17 Sep 2024 main.un.org**
ISIL (Da'esh) & Al-Qaida (1267/1989 Committee)	**253**	**89**	**342**	**UN 1267/1989 list page, updated 9 Jun 2025 main.un.org**
Taliban (1988 Committee)	**135**	**5**	**140**	**UN 1988 list page, updated 30 Jan 2019, main.un.org**
Iran – Annex B to UNSCR 2231	**23**	**61**	**84**	**main.un.org**

Penalties for failure to comply with these requirements are described in Section 2.7 below.

2.3 FREEZING OF ASSETS

Overview

Section 14 of the UNFSA prohibits FIs from dealing with an asset knowing that the asset is owned, controlled or held, directly or indirectly, wholly or jointly, by or on behalf of or at the direction of a DPE. Such assets are defined by Section 5 of the UNFSA as "frozen assets."

Under Section 5 of the UNFSA, an "asset" is very broadly defined. It includes:

> *"funds, property and financial resources of every kind, whether tangible or intangible, corporeal or incorporeal, moveable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including but not limited to currency, bank credits, deposits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit and any interest, dividends, income or value accruing from, generated by or derived from such asset."*

"Dealing," when used in relation to an asset, includes the transfer, conversion, disposition, movement or use of that asset.

The prohibition on dealing with or providing assets or financial services to DPEs (or persons or entities controlled directly or indirectly by DPEs) must be implemented immediately upon identification of a person or entity as a DPE or controlling person, without prior notice to that person or entity. FIs must not inform a customer, their BO(s) or authorised representative(s) that assets will be frozen or assets or financial services will not be provided prior to any taking any such action. This is important because not only is advising, warning or "tipping off" the affected customer itself an offence (which can result in significant penalties), but it can prompt the DPE to move assets out of reach.

Authorisation to Deal With Frozen Assets

Part III of the UNFSA sets out a process for enabling a person to seek authorisation to deal with frozen assets or make an asset or financial service available in certain circumstances. Section 17 of the UNFSA provides that a person may apply in writing to the Prime Minister for such an authorisation, and the Prime Minister may grant such an authorisation upon that application, or upon the Prime Minister's own instigation.

Such authorisations may only be given on certain conditions, namely that the asset is required to meet -

- *a basic expense* (defined in Section 5 of the UNFSA as obtaining foodstuffs; paying rent or mortgage; obtaining medicine or medical treatment; paying taxes; paying insurance premiums; paying public utility charges; paying reasonable professional fees; paying reasonable expenses associated with the provision of legal services; and paying fees or service charges in accordance with laws of PNG for the routine holding or maintenance of a frozen asset);

- *a contractual obligation* (defined in Section 5 of the UNFSA as an obligation whereby a payment is required under contracts or agreements made before the date of the designation and where the payment required does not defeat the object and purpose of the UNFSA); or

- *an extraordinary expense* (defined in Section 5 of the UNFSA as a payment which is not a basic expense or contractual obligation, that the Prime Minister considers necessary and that he considers does not defeat the object and purpose of the UNFSA).

The application must be accompanied by sufficient evidence to support the request and to demonstrate that the above criteria are satisfied. The Prime Minister may authorise the management, or administration of a frozen asset for purposes including, but not limited to, maintaining the value of the asset, but may not grant an authorisation where there are reasonable grounds to believe that the asset or financial service will be used for a purpose other than fulfilling the stated conditions. The Prime Minister may also impose other conditions on any authorisations granted.

Another key element of the authorisation process requires that prior to authorising any dealing with a frozen asset or the making available of an assets or financial service, the Prime Minister must-

- seek any approvals required by, and make any notifications required to, the UNSC or its Committees; and

- consider any communication from a foreign government relevant to the authorisation.

A person may also apply directly to the relevant UNSC Committee through a procedure described on the websites of the Sanctions Secretariat and the U.N. Security Council.[4]

2.4 REVOCATION

A DPE may be removed from the Sanctions Lists (Consolidated List) by the UNSC or one of its Committees, or by the Prime Minister or a PNG court. The Sanctions Secretariat's website noted above provides information regarding the revocation process (also known as "delisting").

Per Section 6 of the UNFSA, a Schedule 1 designation (see Note 1 above) can only be revoked by the UNSC or the relevant UNSC Committee that oversees the particular sanctions program in question. The Prime Minister may submit a request for delisting to the UNSC or its relevant Committee for their consideration and subsequent decision. A DPE can also apply directly to either the U.N.'s Office of the Ombudsperson or Focal Point,[5] depending on the Sanctions List(s) on which the DPE is included.

For Schedule 2 (domestic) designations (DPEs designated under UNSCR 1373), Section 11 of the UNFSA provides the procedures for de-listing (note that currently there are no domestic designations). The Prime Minister is required to periodically review all interim designations, final designations and Prime Ministerial and court re-designations to determine whether the grounds for the designation continue to be satisfied. Where the Prime Minister is of the view that such grounds are no longer satisfied, the Prime Minister, acting on the advice of the National Security Advisory Committee, is required to –

- in the case of an interim designation or Prime Ministerial re-designation, revoke the designation or re-designation; or

- in the case of a final designation or National Court re-designation, make an application to the National Court for it to revoke the designation or re-designation. If the National Court agrees that such grounds are no longer satisfied, it is required to revoke the designation.

The Prime Minister notifies FIs, DNFBPs, and any other necessary persons of any revocations.

2.5 ASSISTANCE FROM THE COMMISSIONER OF POLICE

At times, an FI may suspect that it is holding an asset that is, or may be, owned, controlled or held on behalf of, or at the direction, of a DPE. In this event, Section 16 of the UNFSA provides a process whereby the FI may seek the assistance of the Commissioner of Police in order to help verify that suspicion. The request must be accompanied by details of the asset and the owner or

[4] https://pngsanctionssecretariat.gov.pg/authorization/; https://main.un.org/securitycouncil/en/content/2231/assets-freeze-exemptions

[5] DPEs seeking to be removed from the UNSC's ISIL (Da'esh) and Al-Qaida Sanctions List can submit their request to an independent and impartial Ombudsperson who has been appointed by the U.N. Secretary-General. DPEs on the sanctions list of one of the UNSC sanctions committees, except for individuals inscribed on Al-Qaida Sanctions List can submit such requests either through the U.N.'s Focal Point, which is a mechanism established by the UNSC to facilitate delisting requests from UN sanctions lists, or through their State of residence or citizenship (in this case, PNG).

controller of the asset, if known to the person making the request. The Commissioner of Police is obligated use his best endeavours to assist in making that determination, including providing a written response as soon as is reasonably practicable after receiving the request.

2.6 REPORTING OBLIGATIONS

Under section 40 of the AML/CTF Act, an FI must report to FASU any assets which it holds of a DPE. The report must be made as soon as is reasonably practicable or within 10 working days from the date notification of a designation is received.

An FI must also file a suspicious matter report (SMR) with the FASU without delay whenever it has reasonable grounds to suspect that:

- an asset, transaction or attempted transaction may breach sections 14-15 of the UNFSA (i.e., dealing with or providing assets/services to a DPE); or

- information in its possession may be relevant to detecting, investigating or prosecuting such a breach.

2.7 OFFENCES AND PENALTIES

PNG's sanctions regime will be far more effective if FIs voluntarily comply with their obligations under the UNFSA and AML/CFT Act. This will assist in detecting, deterring and preventing terrorist and proliferation financing, which in turn will contribute to strengthening the safety and financial stability of PNG. However, Sections 14 and 15 of the UNFSA prescribe a broad range of enforcement measures and failure to comply with obligations under the UNFSA or AML/CFT Act will attract heavy penalties, which are summarised below:

Offence	Individual	Company
Dealing with frozen asset(s) (s 14)	≤ PGK 100 000 or 9 years imprisonment	≤ PGK 450,000 or asset value
Making assets available (s 15)	Same	Same
Reckless breach	≤ PGK 50 000 or 5 years imprisonment	≤ PGK 250,000 or asset value

3. ELEMENTS OF AN EFFECTIVE SANCTIONS COMPLIANCE PROGRAM

Because of the above factors, it is critical that each FI establish and maintain an effective sanctions compliance program (SCP). Such a program will consist of the following elements:

- Board and Management Commitment
- Risk assessment
- Internal controls
- Testing and auditing
- Training

3.1 BOARD AND MANAGEMENT COMMITMENT

The success of an FI's risk-based SCP begins with the board of directors (or equivalent policy-making body) and senior management. The commitment and support of the board and management are essential in ensuring that the SCP receives adequate resources and is fully integrated into the FI's daily operations. This commitment and support will also help to legitimize the program, empower the FI's personnel, and promote a culture of compliance throughout the entire organization.

Board Approval of the SCP

The starting point for developing an effective SCP is a written policy approved by the board of directors. The program should contain the following elements:

- policies and procedures for identifying persons and entities that are subject to sanctions, reporting and transfer of information and documents to the responsible compliance officials within the FI, and to the competent governmental authorities as appropriate;

- procedures for maintaining a current list of DPEs and for disseminating such information throughout the FI's domestic operations and, if applicable, its foreign subsidiaries, branches and offices. The procedures should require that all new accounts, including deposit, loan, trust, or other relationships be compared with the sanctions lists when accounts are opened. Established accounts should be compared regularly with the current and updated sanctions lists. Wire transfers, letters of credit, and non-customer transactions, such as funds transfers, should be compared with the sanctions lists before being conducted;

- rules and procedures for the appointment and discharge of officials within the FI who are responsible for implementing the board-approved policy, the powers and obligations of compliance officers and the implementation of the relevant rules;

- requirements for providing training for the compliance officers and employees of the FI whose job responsibilities entail contact with customers who may be subject to sanctions, or for reviewing and analysing information collected by the front-line employees;

- assessment of the FI's sanctions-related risk in relation to its customers, services and products;

- independent testing of the effectiveness of the policies and procedures by internal auditors or an outside party); and

- procedures in relation to enhanced due diligence (EDD) in case of higher risk customers.

The board and senior management should ensure that the FI's compliance unit has sufficient authority and autonomy to deploy its policies and procedures in a manner that effectively controls the FI's sanctions-related risk. As part of this effort, the board and senior management should ensure that there is a direct reporting line between the compliance function and board

and senior management, including routine and periodic meetings between these elements of the FI.

Sanctions Policy Statement

One very effective step in the creation of a strong control culture in this context is for the board of directors and management to issue a policy statement that clearly expresses the FI's commitment to sanctions compliance. The policy statement can be a stand-alone document that specifically addresses sanctions compliance, or part of a broader document that addresses combatting the abuse of the FI's facilities, financial products, and services for the purpose of money laundering, terrorist financing, and criminal activity, or even one that addresses compliance with all laws and regulations to which the FI is subject.

This policy statement should be a summary of "best practice" of the FI's board of directors and senior management, which outlines the FI's policies and procedures and should be communicated to all employees of the FI. It should state the FI's intention to comply with current AML/CFT/CPF legislation as well as provisions and guidelines, in particular the laws and guidelines regarding the identification of customers and the reporting of frozen assets and suspected sanctions evasion, and should cover the items mentioned above.

In the design, update, and implementation of their policy statement, FIs should make extensive use of the domestic legal and regulatory provisions reference above, this Guideline, the Sanctions Secretariat and FASU websites, and the relevant standards from international standard-setting bodies such as the FATF, the Basel Committee on Banking Supervision and the Wolfsberg Group. Examples of those standards include, among others:

- The FATF Standards (2012, latest update June 2025);
- FATF *Guidance for Financial Institutions in Detecting Terrorist Financing*
- Basel Committee publications:
  Customer due diligence for banks
  Internal Controls for Banking Organizations
  Sound management of risks related to money laundering and financing of terrorism.
- Wolfsberg Group:
  Guidance on Sanctions Screening
  Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption

Sanctions Committee

FIs, particularly larger FIs and those with significant cross-border operations, should consider establishing a sanctions compliance committee. A sanctions compliance committee can provide oversight of the SCP and help to ensure that it is effective.

Resources

The board of directors should ensure that the FI's compliance unit(s) receive adequate resources—including in the form of human capital, expertise, information technology, and other resources, as appropriate—that are relative to the FI's breadth of operations, target and

secondary markets, and other factors affecting its overall risk profile. These efforts could generally be measured by the following criteria:

- appointment of a dedicated sanctions compliance officer (SCO);[6]
- the quality and experience of the personnel dedicated to the SCP, including:
  - the technical knowledge and expertise of these personnel with respect to sanctions-related laws, regulations, processes, and actions;
  - the ability of these personnel to understand complex financial and commercial activities, apply their knowledge to these items, and identify sanctions-related issues, risks, and prohibited activities; and
  - efforts to ensure that personnel dedicated to the SCP have sufficient experience and an appropriate position within the FI, and are an integral component to the FI's success;
- sufficient control functions exist that support the FI's SCP, including (but not limited to) IT software and systems, that adequately address the FI's sanctions risk assessment and levels;
- the ability of personnel to report sanctions related misconduct by the FI or its personnel to the board and/or senior management without fear of reprisal;
- the board's and senior management's commitment to discouraging misconduct and prohibited activities, and the potential repercussions of non-compliance with sanctions related requirements; and
- the ability of the SCP to have oversight over the actions of the entire FI, including but not limited to senior management, for the purposes of compliance with the UNFSA and related regulations.

The board and senior management should demonstrate recognition of the seriousness of potential violations of the UNFSA and related regulations, or malfunctions, deficiencies, or failures by the FI and its personnel to comply with the SCP's policies and procedures, and implement necessary measures to reduce the occurrence of apparent violations in the future. Such measures should address the root causes of past apparent violations and represent systemic solutions whenever possible.

3.2 SANCTIONS RISK ASSESSMENT

Another element of an effective SCP is a sanctions risk assessment. It is a good business practice for FIs to conduct a "top-to-bottom" assessment of their sanctions risks, which will

[6] Many institutions designate a single person to oversee all areas of financial crimes or sanctions compliance, but depending on size and complexity of the institution, this may be an individual who focuses exclusively on sanctions compliance, or may be the same person serving in other senior compliance positions.

assist them in developing their sanctions programs. A good risk assessment should:

- be in writing (it can be stored electronically);
- identify and assess the nature and level of TF and PF risks that the FI may reasonably expect to face in the course of its business; and
- be maintained and updated as required to take into account new and emerging risks.

Risks specific to sanctions compliance generally can be defined as *potential threats or vulnerabilities that, if ignored or not properly handled, can lead to violations of the UNFSA or related regulations, and negatively affect an FI's reputation and business*. The main sources of these risks are:

- the FI's customers, supply chain, intermediaries, and counter-parties;

- the products and services that the FI offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and

- the geographic locations of the FI, as well as of its customers, supply chain, intermediaries, and counter-parties.

Some of the key focus items that an FI should consider include:

- **Direct exposure to DPEs.** This is the most obvious risk, and it is what most people think of when they hear the term "sanctions risk."

- **Indirect exposure to DPEs.** This can occur through a variety of channels, such as doing business with a company that is owned or controlled by a DPE, and is particularly problematic in cases where DPEs attempt to hide their involvement in transactions or business relationships in order to evade sanctions (see Section 1.5 above).

- **Failure to properly screen customers and transactions.** This can lead to inadvertent violations of sanctions, even if the FI is not directly exposed to DPEs.

- **Inadequate training for employees.** Employees who are not properly trained on sanctions compliance are more likely to miss situations that could lead to violations of the UNSCA and related regulations.

While there is no "one-size-fits all" formula for a risk assessment, the exercise should generally consist of a holistic review of the FI's operations and assess its touchpoints to the outside world. This process allows the FI to identify potential areas in which it may, directly or indirectly, engage with DPEs. Risk assessments and sanctions-related due diligence are also important during mergers and acquisitions, particularly in scenarios involving foreign entities.

A good risk assessment will:

- identify *inherent risks* (the degree of risk in a given category before the implementation of mitigating controls) in order to inform risk-based decisions and controls;

- assess the *effectiveness of controls* that are instituted to mitigate those inherent risks; and

- determine the overall *residual risk* (the risk that remains after controls are put in place to reduce inherent risk).

Each FI will need to design its own risk assessment based on its particular circumstances. A suggested framework is presented in **Appendix 1**.

3.3 INTERNAL CONTROLS

An effective SCP should include internal controls containing the following elements:

- **Written policies and procedures outlining the SCP.** These policies and procedures should be relevant to the FI, capture the its day-to-day operations and procedures, be easy to follow, and be designed to prevent employees from engaging in misconduct.

- **Effective implementation of the internal controls.** This should adequately address the results of the FI's risk assessment and profile. The internal controls should enable the FI to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the FI any transactions or activity that may be prohibited by the UNFSA or related regulations. To the extent that information technology solutions form part of the FI's internal controls, the FI should ensure that it has selected and calibrated the solutions in a manner that is appropriate to address its risk profile and compliance needs. The FI should routinely test the solutions to ensure effectiveness.

- **Appointment of personnel responsible for integrating the policies and procedures into the daily operations of the FI.** This process entails consultations with relevant business units, and ensuring that the FI's employees understand the policies and procedures.

- **Enforcement of the policies and procedures** through an effective compliance function headed by a designated SCO, as well as internal and/or external audits.

- **Recordkeeping policies and procedures** to document adherence to the requirements of the UNFSA and related regulations.

- **Clear communication** of the policies and procedures to all relevant staff, including personnel within the SCP program, as well as relevant gatekeepers and business units operating in high-risk areas (e.g., customer acquisition, payments, sales, etc.) and to external parties performing SCP responsibilities on behalf of the FI.

- **Corrective action** upon learning of any weaknesses in the internal controls, to identify the root cause of the weakness institute remedial action.

The following sections highlight some of the most critical internal control mechanisms.

Customer Due Diligence and Screening Procedures

The cornerstone of a strong SCP is the ability of an FI to *know its customers,* in order to be satisfied that a customer (or potential customer) is not a DPE, or associated in any way with a DPE. The AML/CFT Act sets out the CDD obligations in Part II, Division 2 (Sections 15 to 33). Specifically:

- Subdivision 1 – General due diligence requirements (Sections 15 to 19);
- Subdivision 2 – Customer due diligence requirements (Sections 20 to 29);
- Subdivision 3 – Customer due diligence requirements for electronic funds transfers (Sections 30 to 33);

Section 8 of the FASU AML/CFT Guidance for FIs elaborates on this topic in the AML/CFT context; however, there are steps that should be taken *in addition to baseline customer due diligence (CDD) procedures and other anti-money laundering (AML) controls* which can be critical for detecting, stopping, and reporting attempted or suspected sanctions evasion. These additional steps involve *screening*.

Screening refers the comparison of one string of text against another to detect similarities that would suggest a potential match. If a match is detected, and the FI maintains accounts, or otherwise holds or controls funds and other assets for DPEs (or any entity owned or controlled by DPEs, or acting on their behalf of for their benefit), FIs should immediately:

- not deal with those funds and other assets, per Section 14 of the UNFSA;
- not make funds and other assets available to or for the benefit of DPEs, per Section 15 of the UNFSA;
- report the situation to the FASU as required by Section 40 of the AML/CFT Act; and
- if the situation warrants, investigate further as detailed below.

FIs will typically utilize two main screening techniques:

- customer/name screening to identify DPEs during onboarding and also at other crucial stages of the customer relationship; and
- transaction screening, which seeks to identify transactions that involve DPEs.

Many FIs use sanctions screening software that is available from commercial vendors. The type and degree of sophistication will depend on the type and complexity of the FI; a small stand-alone FI that mainly serves established local customers operating in the domestic market will have very different screening needs than a large FI that is part of a financial group with customers and transactions spanning many jurisdictions.

The Screening Process

The screening process generally consist of the following steps:

- **Data collection and preparation:** This entails gathering by the front-line business units of relevant customer data, which typically includes names, addresses, and identification numbers, as well as transaction details and BO information. Strictly speaking, this is not part of the screening process; however, it is critical to the proper functioning of that process. Customer data must be accurately entered and maintained. Poor data quality and integrity can have a severely negative impact on the ability of the FI to know its customers and conduct customer due diligence. This data therefore must be standardized and formatted for efficient screening.

- **Screening against sanctions lists:** The prepared data is screened by one or more sanctions analysts against the U.N. Consolidated List published by the Sanctions Secretariat or directly against the UNSC lists. This screening process can involve exact matches, fuzzy logic (finding partial matches with imprecise data), or phonetic matching (matching names that are pronounced the same) to identify potential matches. Larger FIs may find it helpful to have the initial screening performed by two different analysts without communication between them. If their conclusions are different, it is a reliable indication that referral to a more experienced senior analyst is necessary. Regardless of whether the initial review is performed by one analyst or two, it is a good practice to have this initial step reviewed by a more senior analyst whenever possible.

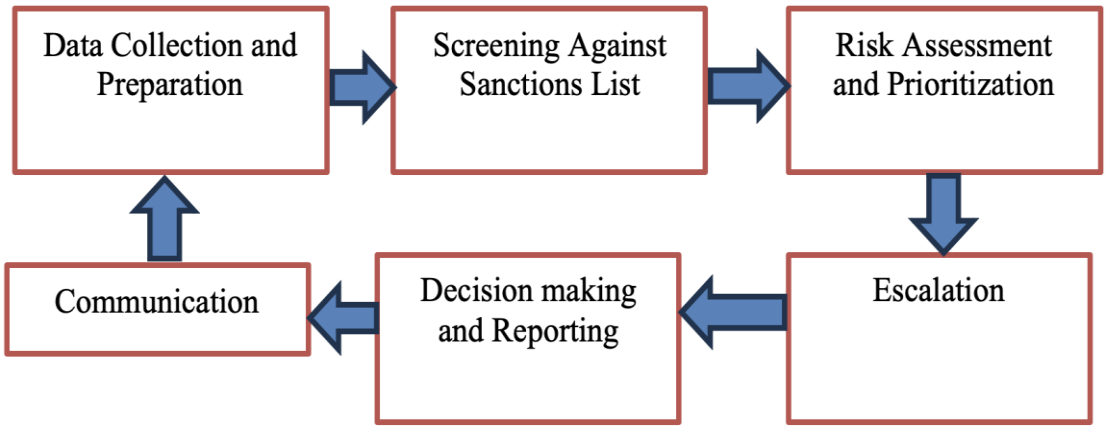
- **Risk assessment and prioritization:** Risk assessments are conducted on any identified matches. The potential risk associated with each match is evaluated based on factors such as the type of transaction and the customer's risk profile. Matches should be prioritised for further investigation.

- **Escalation:** High-risk matches should undergo a more thorough investigation including additional research and due diligence, and, potentially, contacting relevant authorities. This step determines whether the match is a true positive or a false positive. Typically, this step would be conducted by a more experienced analyst.

- **Decision-making and reporting:** Based on the investigation's findings, a decision is made regarding the match. If the match is a true positive, the decision is communicated to the relevant business line and appropriate action is taken, such as freezing assets, blocking transactions, or reporting to FASU. False positives are documented and cleared. Typically, this decision will be taken by a senior member of the sanctions compliance function, such as the FI's SCO or an experienced member of the compliance staff with delegated authority.

Of course, the details of the above scenario can vary depending on the size and risk profile of each FI. Smaller FIs might not have the resources or personnel to institute multiple layers of review; in this case the FI will need to ensure that the person(s) performing the initial screening are thoroughly competent regarding use of the Consolidated List and the criteria for FI action when DPEs are identified.

The following figure depicts the screening process:



Customer Name Screening

FIs must have a system in place to screen customers during on-boarding and through the life cycle of the customer relationship. This also includes directors and BOs of corporate customers, and any other parties with access to the account. At a minimum, screening should take place when establishing a new relationship, and at regular intervals either upon a trigger event (such as a change in directors or ownership) or when a sanctions list changes.

Sanctions screening should be a top priority after the initial risk assessment when onboarding a customer or third party. In addition, FIs should that ensure existing customers and third parties are screened on a regular basis. Possible matches should be addressed urgently, with clearly defined processes for escalation. Some of the main issues include:

Name variations

This is an extremely important part of the screening process. FIs should ensure that their screening system can handle name variations. Some of the more common issues likely to be encountered are summarized in **Appendix 2**.

Issues Regarding Birth Dates

Dealing with birthdates can present challenges for two main reasons:

- High risk individuals often do things to obscure their real date of birth.

- In many jurisdictions, birth certificates do not exist. Some people may not know their exact date of birth, and even if they do, they may not have any documentation to verify it. For some individuals, dates of birth may simply be guessed or interpreted based on other characteristics such as when they went to school or when they got married (which would be accurate to within a few years at best).

In the cases where an exact birthdate is not available, birthdate filters should be set to match the level of risk. For example, an FI might filter its screening results against a "politically exposed person" ("PEP") filter with a configuration of plus or minus one year. This will allow the FI to narrow its screening hits to the most likely results and help to balance resources spent while still allowing for a risk-based approach. If the FI screens for adverse media, this can be

a larger range such as plus or minus four years (depending on the FI's risk appetite). FIs should screen against law and regulatory enforcement data with a much wider net, such as plus or minus five or six years.

Finally, as with any filter, there is always a possibility of false negatives. FIs should set their filters to ensure that they are not missing any high-risk false negatives. Some jurisdictions have reliable birthdate information, so FIs can use a tighter date range. For other high-risk jurisdictions where birthdate information cannot be trusted, a wider threshold will be necessary.

Transaction Screening

Each customer or potential customer, and each incoming and outgoing transaction should be screened for a potential match with the Sanctions List. This is the first, and most critical step. Screening prior to completing a transaction is known as *real-time screening* and is the most widely used. In transaction monitoring, some of the most common screening data points include:

- Parties involved (remitter, beneficiary, other financial institutions involved in the transaction, intermediaries);
- Vessels and International Maritime Organization (IMO) numbers (unique identifier number assigned to each vessel) – especially relevant for DPRK;
- Bank names, bank identifier codes (BIC) and other routing codes; and
- Free text fields (e.g., payment reference).

FIs should pay particular to those data points within the transactional process where information could be modified or removed to undermine screening controls, for example evidence that information has been stripped from the transaction, or the transaction exhibits signs of sanctions evasion techniques.

Updating Sanctions Records

An FI's internal controls should include policies, procedures, and processes for timely checking for updates of the list of DPEs published by the Sanctions Secretariat, and disseminating any updates to all relevant FI personnel, including to its branches and subsidiaries.

Controls Pertaining to Asset Freezes

Once assets are frozen, they should be placed in a separate account specifically designated to hold frozen assets. The screening process should clearly identify the FI personnel with the authority to approve the freezing of assets, indicate how the decision to freeze assets will be identified to other FI staff, and include a procedure for maintaining a written record of the determination to freeze the asset(s).

More information on recordkeeping regarding frozen assets is provided below.

Controls Pertaining to Authorisations

An FIs' internal controls should contain provisions to ensure that they do not apply the prohibitions to persons and entities that have been issued such an authorisation by the Prime Minister or by the UNSC or one of its Committees (described in Section 2.3 above). The controls should:

- indicate how unfrozen assets will be identified to other FI staff, including all relevant information (e.g., which assets of a given DPE are unfrozen and which, if any, remain frozen and any conditions that may be attached to the authorisation);

- include a procedure for maintaining a written record of the determination to unfreeze the asset(s), and for ensuring that the list of unfrozen assets remains current and accurate;

- require written records to document any use of unfrozen assets in order to demonstrate that any such use in in line with the authorisation granted by the Prime Minister or the UNSC or relevant Committee, including compliance with any conditions that may accompany the authorisation.

Resolving False Positives

False positives are potential matches to listed persons and entities, either due to the common nature of the name or to ambiguous identifying data, which prove not to be matches on examination. This can occur for a number of reasons:

- **Overly sensitive systems:** Some systems might be set up capture too much information, triggering alerts for a wide range of customers or transactions that are actually legitimate.

- **Data quality issues:** Inaccurate or incomplete data can lead to incorrect matches and flags.

- **Outdated systems:** Older systems may rely on older matching methods and rules that are no longer effective.

- **Similar names or patterns:** International naming conventions or common transaction patterns can lead to false matches with individuals or entities on sanctions lists (see **Appendix 2**).

False positives can cause a number of problems for FIs:

- **Waste of resources:** False positives consume significant resources, including time, personnel, and financial resources, for investigations that ultimately prove unnecessary.

- **Delays in legitimate customer onboarding:** Until all screening procedures are completed and a decision is made, the FI cannot onboard a customer.

- **Business disruption:** False alerts can disrupt legitimate business operations, causing delays in transactions and potentially damaging relationships with legitimate customers.

- **Erroneous freezing of assets:** One of the unfortunate consequences of false positives is that a person or entity might mistakenly have its assets frozen. Where a person or entity believes that their assets have been frozen in error, they should immediately contact the asset holder (the FI or DNFBP) directly.

- **Obstruction of actual threats:** If a high number of false positives occur, the sheer volume of matches could be so high that some actual positives might be missed. This can result in under-reporting of information to the FASU, which in turn can lead to fines and penalties.

- **Reputational damage:** False positives can harm the reputation of individuals and businesses, leading to unnecessary scrutiny and potential reputational damage.

False positives can never be completely eliminated. They can, however, be significantly minimised. FIs can take several steps to accomplish this:

- **Regular review***:* FIs should periodically review and optimize their transaction monitoring systems to balance sensitivity with accuracy.

- **Data quality improvement:** FIs should invest the time and resources to improving data quality and ensuring that their systems have access to accurate, complete and up-to-date information.

- **Implement "whitelisting:"** FIs should consider creating lists of known legitimate customers and transactions to prevent them from being flagged unnecessarily.

- **Collaboration and information sharing:** FIs should promote collaboration between different departments (and where applicable, entities within the same group) to share insights and improve the effectiveness of customer identification efforts.

- **Use sophisticated algorithms:** FIs should employ more advanced matching algorithms that can distinguish between true and false positives.

- **Use entity resolution:** FIs should implement entity resolution to match multiple pieces of information to identify and resolve false positives more efficiently.

- **Leverage AI:** FIs may use AI-powered tools to reduce false positives and improve the accuracy of screening.

- **Training and awareness**: FIs should provide training to employees on how to identify and respond to false positives effectively.

In some cases, additional follow-up measures may be necessary. While a potential match does not always indicate an actual match, where the above steps are inconclusive, the issue should be investigated further, and either confirmed or dismissed based on that investigation. Such follow-up techniques can include:

- Communicating compliance expectations to customers on a risk basis, including informing them that they may not use their accounts to do business with DPEs. This may also include sharing the list of DPEs with customers, especially customers engaged in import-export activity, manufacturing, or any other relevant business lines.

- Sending questionnaires, on a risk basis, to customers known to deal in high-risk jurisdictions or other parties to better understand their counterparties.

- Using open-source information and past transactional activity to inform due diligence and to conduct proactive investigations into possible sanctions and export control evasion.

- Undertaking proactive investigations into suspected sanctions evasion within the unit or department of the FI that deals with issues concerning financial crimes. These often involve post-transaction reviews for typologies, networks, and/or suspicious activity, as opposed to real-time, list-based screening. Sanctions-related information (e.g., interaction with listed entities prior to their designation as such) can serve as an input for these investigations. The results of these investigations could then be used to further identify risky customers and other sanctions related risks.

- Using information received through requests for information from PNG and global correspondent banks, as well as data from commercial service providers or public data sources such as trade and customs data, to inform due diligence and conduct proactive investigations.

- When appropriate, obtaining attestations from high-risk customers that they do not engage in any sales or transfers or otherwise conduct any transactions with DPEs.

- Taking appropriate mitigation measures for any customers or counterparties engaged in high-risk activity or who fail to respond to requests for information regarding activity of concern. These measures include restricting accounts, limiting the type of permissible activity, exiting relationships, and placing customers or counterparties on internal "do not onboard" or "do not process" watchlists.

- Incorporating risks related to DPEs into sanctions risk assessments and customer risk-rating criteria. This includes updating jurisdictional risk assessments as appropriate.

- Implementing enhanced trade finance controls related to the specified items, including monitoring information collected as part of documentary trade.

Beneficial Ownership

One of the most critical aspects of customer identification is knowing the *beneficial owner* (BO) of an account or of a legal entity or legal arrangement that is or seeks to become a customer. Section 5(1) of the AML/CFT Act defines a BO as a natural person who –

- has ultimate control, directly or indirectly, of a customer; or

- ultimately owns, directly or indirectly, the customer.

According to FASU Guidance, "control" includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, where or not having legal or equitable force and whether or not based on legal or equitable rights. This includes exercising control through the capacity to make decisions about financial and operating policies. "Owns" means ownership, either directly or indirectly, of 25% or more of a person or unincorporated entity.[7]

Beneficial ownership is easy to define, but can be extremely challenging to identify in practice. FIs need to be extremely diligent to ensure that they know who is actually controlling their customers or potential customers, not just who the nominal owners are. **Appendix 3** provides detailed guidance on this issue.

Distinctions between BO Status and Ownership for DPE purposes

For purposes of determining control for sanctions screening purposes, the BO criteria described **in Appendix 3** is helpful. However, there are some important differences that must be kept in mind:

- A BO is always a natural person; a DPE can be either a natural or legal person.

- The numerical tests/thresholds for determining ownership are different. In PNG, 25% is the relevant ownership threshold for BO identification. Based on international practice, 50% is more typical in for determining DPE status for an entity.

When assessing ownership of a given entity, the aggregated ownership of the entity should be taken into account. For example, if one DPE owns 30% of the entity and another DPE owns 25% of the entity, the entity should, in principle, be considered as owned by DPEs.

Sanctions Compliance Officer

An effective sanctions compliance program necessitates a compliance function within each FI. According to the AML/CFT Act, FIs are required to appoint an AML/CFT compliance officer. Many FIs may find it convenient to assign sanctions compliance duties to the AML/CFT compliance officer as part of that officer's overall duties. Larger FIs may choose to have a SCO to be responsible specifically for the administration and management of the FI's SCP. Regardless of the structure, the SCO should:

- have thorough knowledge of sanctions laws and regulations, relevant U.N. Security Council resolutions, and sanctions-related recommendations of international standard-setting bodies such as the FATF;

- satisfy the fit and proper criteria issued by FASU or the FI's regulatory authority;

- have direct access to the board of directors and senior management of the FI without any restrictions in order to apprise the board of directors and senior management of ongoing compliance with the UNFSA, related regulations and the SCP; and

[7] FASU Guidance for Financial Institutions on their Obligations under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (No. 1 of 2019) Section 8, page 25.

- possess strong writing ability and communications skills in order to ensure that reports (both internal, to the board and senior management and external, to regulatory and law enforcement authorities) are complete, clear, and accurate, and that communications with the regulatory and law enforcement authorities will be effective.

Case study: Customer Due Diligence

ABC Bank, a mid-sized PNG bank, is approached by a representative of XYZ Enterprises, which is incorporated and has its principal place of business in a foreign jurisdiction. XYZ wishes to establish a customer relationship with ABC Bank. ABC Bank should take the following steps in accordance with its sanctions compliance program to avoid contravening the UNFSA and related regulations:

- Confirm that the person purporting to represent XYZ Enterprises is in fact authorized to so do (such as by reviewing a power of attorney, resolution of XYZ's board of directors, or similar document that gives this person the authority to act for XYZ Enterprises).
- Review the PNG Sanctions Secretariat website for any relevant sanctions compliance material related to the country in which XYZ Enterprises operates. This includes checking for updates on sanctions regulations and any additional guidance provided by the Sanctions Secretariat.
- Undertake a check on XYZ Enterprises against the list of DPEs available on the UNSC website, email updates from the Sanctions Secretariat and its website, to ensure that XYZ Enterprises is not listed as a DPE.
- Evaluate the risk associated with the prospective customer relationship by reviewing the details of XYZ Enterprises, including the jurisdiction(s) in which it operates (i.e., to determine whether any of them are high-risk jurisdictions), the type of business it conducts, and any known business connections. This will help in assessing whether the relationship might inadvertently involve a DPE.
- Request additional details from XYZ Enterprises, including its registration information and ownership structure. Check any parent companies, intermediate holding companies and ultimate beneficial owners against the Sanctions Secretariat's list of DPEs. This helps confirm that XYZ Enterprises is not linked to any DPEs.
- If any initial checks or additional information raise concerns about potential links to DPEs, defer establishing the relationship and seek further clarification or advice before proceeding.
- If necessary, obtain independent legal advice to provide guidance on the necessary steps to verify whether the proposed customer relationship would be permissible under the UNFSA and related regulations.
- Maintain detailed records of the steps taken, including the screening process, any legal advice obtained, and communications with XYZ Enterprises. This documentation serves as proof of the Bank's due diligence.

After conducting the screening and obtaining independent legal advice, the Bank confirms that while XYZ Enterprises is incorporated in a high-risk jurisdiction, it is not a DPE, is not owned or controlled by a DPE, and is not involved in any business relationships with DPEs. It therefore concludes that establishing the customer relationship would not involve a contravention of the UNFSA.

Recordkeeping and Reporting

Section 40 of the AML/CFT Act requires FIs to report to the FASU any assets that they hold of a DPE. The report must be made as soon as is reasonably practicable or within 10 working days from the date notification of a designation is received.

A FI's internal controls should include policies, procedures, and processes regarding frozen assets, including the procedure for escalating suspected positive matches (described above regarding the screening process), identification of the person within the FI responsible for submitting the required reports to the FASU, and the steps in the process for doing so. Records should include:

- the amount of frozen assets;
- the ownership of those assets;
- interest paid on any frozen accounts;
- a description of any transaction associated with frozen assets, including:
  - the type of transaction;
  - any persons, including FIs, participating in the transaction and their respective locations;
  - to the extent known, any customers, beneficiaries, originators, letter of credit applicants, and their banks; intermediary banks; correspondent banks; issuing banks; and advising or confirming banks; and
  - any reference numbers, dates, or other information necessary to understand the transaction;
- written documentation of the FI's decision to freeze the assets, including the date the assets were frozen, the approving official within the FI (normally the SCO or other person with delegated authority), copies of any relevant documentation supporting the decision, and any other communications with, or information received from, any regulatory authority regarding the assets; and
- documentation regarding any decision to unfreeze assets (see Section 2.3 above).

When an FI acquires or merges with another FI, both FIs should take into consideration the need to review and maintain such records and information, paying particular attention to the need for consistency of reporting format and avoidance of duplication.

3.4 INDEPENDENT TESTING AND AUDITING

FIs should have their SCPs audited by an independent party on a regular basis. In large and complex FIs, the independent testing (audit) will normally be conducted by an internal audit department; smaller entities, which might not have the resources to support a formal full-time internal audit department, might use outside auditors, consultants, or other qualified independent parties. This is acceptable, provided that the outside audit provider is held to the same quality standards as an in-house function would be. The important thing is that the persons doing the testing must not be involved in other sanctions-related functions such as

training or developing or approving the FI's sanctions policies and procedures. Such involvement may present a conflict or lack of independence, which could taint the testers' findings and compromise their ability to give honest and objective advice to the board and senior management about how the sanctions compliance program is functioning.

There should be a formal document (such as a charter or terms of reference) that clearly sets out the duties and responsibilities of the internal audit function regarding sanctions compliance. The persons conducting the testing should be appointed and dismissed by the FI's board of directors and should report directly to the board or to a designated board committee (preferably the audit committee).

While the frequency of independent audits is not specifically defined in UNFSA or the FASU Guidelines for FIs, it is a good business practice to conduct independent testing generally every 12 to 18 months, commensurate with the FI's risk profile. Testing should address:

- the content of the FI's sanctions policies and procedures and their overall implementation;
- the FI's sanctions risk assessment for reasonableness given the FI's risk profile (products, services, customers, entities, and geographic locations);
- the effectiveness of the FI's customer and transaction screening systems;
- the board's and management's efforts to remedy any violations and deficiencies noted in previous audits and supervisory inspections, including progress in addressing outstanding corrective actions required by the supervisory authority, if applicable;
- the FI's staff training for adequacy, accuracy, and completeness;
- an assessment of the reporting process to the FASU, including a review of filed or prepared reports to determine their accuracy, timeliness, and completeness.

The audit report should document the audit scope, procedures performed, transaction testing completed, and overall findings. Any violations, policy or procedures exceptions, or other deficiencies noted during the audit should be included in an audit report. The board or designated committee and the audit staff should track audit deficiencies and document corrective actions. All audit documentation and work papers should be available for review by the supervisory inspectors.

3.5 TRAINING

A sanctions program cannot be effective if an FI's personnel do not understand the requirements and how to comply with them. It is essential that all personnel whose function requires sanctions knowledge are appropriately trained.

Training should:

- include legal and regulatory requirements and the FI's SCP;
- be tailored to specific job responsibilities;
- be provided to all new staff as soon as possible following on-boarding;

- be provided annually on a “refresher” basis;
- be provided by instructors (preferably including the FI’s SCO) who are thoroughly familiar with the UNFSA, AML/CFT Act, relevant UNSC Resolutions and recommendations of international standard-setting bodies (e.g., FATF);
- include examples and real-world case studies of sanctions evasion techniques;
- describe the FI’s process for detecting suspected sanctions evasion and escalating these concerns to appropriate sanctions personnel within the FI, as well as reporting to the FASU; and
- reinforce the importance that the board and senior management place on sanctions compliance.

FIs should document their training programs. Training and testing materials, the dates of training sessions, and attendance records should be maintained. Employee knowledge based on the training should be checked and serious deficiencies should be remedied. The board of directors should ensure that sufficient resources are devoted to sanctions-related training.

Some small FIs may not have the capacity to develop in-house training programs themselves. In such cases, the training function can be outsourced to a reputable outside training organization. However, the FI must have written policies and procedures regarding the content of the training as outlined above, and means to ensure the reliability of the persons providing the training. The FI itself remains responsible for ensuring that effective training is provided.

Key contacts

Office	Purpose	Contact
Sanctions Secretariat	List updates, licences, and public guidance	mailto:pngsanctions@pmnec.gov.pg
FASU (Bank of PNG)	Suspicious Matter Reports	mailto:fasu@bankpng.gov.pg

REFERENCES

Alessa, Inc., *How to Test Your Sanctions and Watch List Screening Software*, *https://alessa.com/wp-content/uploads/2020/06/How-To-Test-Sanctions-Screening-Software.pdf*

Australian Department of Foreign Affairs and Trade, Sanctions Office, *Sanctions Compliance Toolkit* https://www.dfat.gov.au/international-relations/security/sanctions/guidance/sanctions-compliance-toolkit

Mauritius National Sanctions Secretariat, *Guidelines on the Implementation of Targeted Financial Sanctions Under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019* https://www.bom.mu/financial-stability/supervision/guidelines/guidelines-implementation-targeted-financial-sanctions-under-united-nations

European Union Best Practices for the Effective Implementation of Restrictive Measures https://data.consilium.europa.eu/doc/document/ST-11623-2024-INIT/en/pdf

Jyoti Maheshwari, *Minimising False Positives in Sanctions Screening* (2024), https://rapidaml.com/articles/minimising-false-positives-in-sanctions-screening/

Marcus Tinedo, *Best Practices to Implement a Sanctions Compliance Program in International Banking* (2019)

Sanctions Secretariat of Papua New Guinea, https://pngsanctionssecretariat.gov.pg

U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), *A Framework for OFAC Compliance Commitments* https://ofac.treasury.gov/media/16331/download?inline

U.S. Federal Financial Institutions Examination Council (U.S.) *Bank Secrecy Act/ Anti-Money Laundering Examination Manual* (2014) https://bsaaml.ffiec.gov

Wolfsberg Group, *Guidance on Sanctions Screening* https://db.wolfsberg-group.org/assets/4b6c2db6-696d-492e-bdd5-c51552708597/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

Wolfsberg Group, *Financial Crime Principles for Correspondent Banking* https://db.wolfsberg-group.org/assets/d39a5072-7fb6-4e31-9a87-9e54021ce71f/Wolfsberg%20Correspondent%20Banking%20Principles%202022.pdf

Wolfsberg Group, *Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption* https://db.wolfsberg-group.org/assets/3deb66d7-6aca-490c-bcd9-c1a3d34a807b

APPENDIX 1
SUGGESTED FRAMEWORK FOR CONDUCTING A SANCTIONS RISK ASSESSMENT

I. Overview

A good risk assessment will:

- identify *inherent risks* (the degree of risk in a given category before the implementation of mitigating controls) in order to inform risk-based decisions and controls;

- assess the *effectiveness of controls* that are instituted to mitigate those inherent risks; and

- determine the overall *residual risk* (the risk that remains after controls are put in place to reduce inherent risk).

II. Inherent Risk

Measuring inherent risk provides an FI with an initial "heat map" to identify where resources should be deployed to bring risk down to an acceptable level. An effective risk assessment generally quantifies the level of inherent risk by adopting uniform definitions and assigning point values for each risk level.

Customer Risk

Section 8 of the FASU AML/CFT Guidance for FIs suggests categories that can be used by FIs to determine their vulnerability to ML/TF risk from customer risk standpoint, and this can also be used in the sanctions context. These categories are:

- **Low risk persons or entities** – these are generally individuals and entities whose identities and sources of wealth can be easily identified, and whose transactions conform to their customer profile (for example, salaried employees and persons with low value credit card accounts).

- **Medium risk persons or entities** – these are generally individuals and entities whose business activities may involve varying factors around the person or entity, including:
  - customer profile, background, country of origin;
  - sources of wealth and funds;
  - nature and location of activity; and
  - substantial dealings with government agencies or departments.

- **High risk persons or entities** – these are generally individuals and entities that engage in the following activities:
  - money changers, bullion dealers, money transfer agencies, payday lenders;
  - jewelry or gold dealers;
  - gaming establishments, nightclubs, bars;

- non-resident customers;
- high net worth individuals;
- trusts, charities, non-government organizations including those receiving donations;
- companies having close family shareholding or beneficial ownership;
- politically exposed persons;
- law firms, real estate agents and other entities that operate trust accounts through which customers' funds may be moved anonymously; and
- known criminals or those with dubious reputations as per public information available, or individuals who are known to have been exited by other financial institutions, etc.

To determine its inherent customer risk, an FI should review its customer list and determine the proportion of its customers that fall into the high-risk category. The more high-risk customers a FI has, the higher the sanctions risk it is potentially exposed to. The FI should also consider the approximate volume of transactions or business generated by such customers. FIs often find it useful to assign a risk level to each customer, ranging from "low" (1) to "high" (5). An FI with only a small number or percentage of high-risk customers will generally run a low customer risk, while an FI that has a higher number or percentage of such customers should consider itself as having a high customer risk exposure.

In addition to customers' business activities, FIs should consider the jurisdictions of which their customers are citizens or residents. An FI with very few or no customers from high-risk jurisdictions will generally run a low customer risk, while an FI that has many such customers should consider itself as having a high customer risk exposure. Clients from low-risk countries would be considered low-risk customers, while customers from high-risk countries would be considered high-risk customers. A potential useful tool for determining whether a country falls into the "high-risk" category is the "Know Your Country" website, https://www.knowyourcountry.com. This organization maintains risk ratings for more than 200 countries in several AML/CFT and sanctions categories and is updated periodically.

Using this information, FIs can determine their customer risk. The following table provides a suggested range of assigned values for inherent customer risk.

Level of inherent risk regarding customers	Potential exposure to sanctions risk	Suggested assigned value
High	High – Indicates that a large portion of the FI's customer base involves high-risk customers.	5
Medium-High	Somewhat higher than moderate – Indicates that a slightly higher than a moderate portion of the FI's customer base involves high-risk customers.	4
Medium	Moderate – Indicates that a moderate portion of the FI's customer base involves high-risk customers.	3
Medium-Low	Less than moderate – Indicates that a less than moderate portion of the FI's customer base involves high-risk customers.	2
Low	Negligible – Indicates that only a small portion of the FI's customer base involves high-risk customers.	1

To illustrate how this would work in practice, assume that an FI has 100 customers, having the following risk scores:

- 10 at risk level 1
- 20 at risk level 2
- 50 at risk level 3
- 10 at risk level 4
- 10 at risk level 5

For each of these levels, the FI would multiply the risk level by the number of customers:

- 10 at risk level 1 = 10
- 20 at risk level 2 = 40
- 50 at risk level 3 = 150
- 10 at risk level 4 = 40
- 10 at risk level 5 = 50

  TOTAL 290

The overall total (290) of this calculation would be divided by the total number of customers (100). The resulting risk score for this element would be 2.9, which would be rounded to the nearest whole number (3), indicating a medium risk level for customer risk.

Country/Geographic Risk

Even if an FI's customer is not a citizen or resident of a high-risk jurisdiction, or incorporated in such a jurisdiction, the FI could still be exposed to country risk if its customers do business in, or engage in transactions with citizens or residents of such jurisdictions. In addition, the FI's supply chain, intermediaries, and counter-parties can have an impact on its level of sanctions risk. For example, if an FI's counterparty or supplier is doing business with a DPE, the FI itself could unwittingly become part of the process. If an FI has a branch or subsidiary in a foreign jurisdiction, or is itself a branch or subsidiary of a foreign FI, it needs to be aware of the business environment in which that FI operates.

FIs that have cross-border operations need to be aware of the sanctions risks that these operations can entail. To analyse country risk, FIs should take into consideration whether they have business dealings with countries that:

- have weak or ineffective AML/CFT/sanctions regimes, or have borders with such countries;
- have a high degree of organized crime, particularly drug-related crime, human trafficking or smuggling;
- have a high degree of corruption or bribery;
- are in a conflict zone, or border a conflict zone;
- have significant terrorism activity;

- are conduit countries (countries such as the Netherlands, the U.K., Switzerland, Singapore and Ireland that have advanced legal and tax systems designed to enable corporations to route funds from high tax locations to offshore financial centres (OFCs) that offer tax advantages or a high degree of secrecy);

- have been identified by a credible source (such as the FATF) as high risk for ML/TF predicate offenses; or

- have otherwise been identified by a credible source as having a high level of ML/TF/sanctions risk.

If the answer to any of these questions is "yes," the FI should quantify the number of such countries with which it does business. The more high-risk countries where an FI has activities, the higher the sanctions risks that the FI is potentially exposed to. An FI with only domestic activities will generally run a low country risk, an FI that is active in 1-5 high-risk countries will run a medium country risk, and an FI that is active in more than 5 high-risk countries should consider itself as having a high country risk. "Having activities" or "being active" could consist of:

- having a branch or subsidiary in a high-risk country;

- conducting cross-border transactions;

- having customers that are residents or citizens of, or have legal tax domicile in, high-risk countries;

- having customers (regardless of whether they are citizens or residents of PNG) that use the services of the FI to conduct business with persons in high-risk countries (this could involve trade finance, purchasing/selling/importing products, sending payments to or receiving payments from, sources in high-risk countries); or

- having BOs or controlling persons (whether natural or legal persons) that are citizens or residents of, or are incorporated, have their principal places of business, or have legal tax domicile in high-risk countries.

Again, the "Know Your Country" website referenced above is helpful here. The following table provides an example of an inherent risk rating for country/geographic risk:

Level of inherent risk regarding customers	**Potential exposure to ML/TF**	**Suggested assigned value**
High	High – Indicates that the FI is active in more than 5 high-risk jurisdictions.	5
Medium-High	Somewhat higher than moderate – Indicates that the FI is active in 4 or 5 high-risk jurisdictions.	4
Medium	Moderate – Indicates that the FI is active in 2 or 3 high-risk jurisdictions.	3
Medium-Low	Less than moderate – Indicates that the FI is active in 1 high-risk jurisdiction.	2
Low	Negligible –Indicates that the FI is not active in any high-risk jurisdictions.	1

Products/Services Risk

An FI should analyse and evaluate its products and services as part of its sanctions risk assessment. FIs should ask the following questions:

- What sort of services does the FI offer?
- Have any of these products/services been identified by the legislation of PNG or by governmental authorities as presenting heightened sanctions risk?
- Have any of these products/services been identified as presenting heightened sanctions risk by international guidance?
- Do any of these products/services support physical cash deposits and/or withdrawals?
- Can any of these products/services be redeemed or traded for cash? Are they highly liquid? Do they support early redemption, conversion to cash or equivalent value?
- Do any of these products/services provide international funds transfer capability?
- Does the FI's business facilitate products and services prescribed under U.N. sanctions?
- Do any of these products/services support transactions that can be conducted remotely (e.g., via the internet) or without interaction with FI personnel?
- Do any of these products/services allow high-value, high-volume and high-velocity transactions?
- Do any of these products/services operate using commission-based remuneration?
- Do any of these products/services support the pooling of funds and investments (e.g., a trust account or customer account)?
- Are any of these products/services targeted to offshore customers (e.g., foreign trusts)?
- Do any of these products/services support payments to/from third parties or non-customers?

If the answer to any of these questions is "yes," the FI should determine the volume or percentage of its products or services that fit that description. This should be factored into the determination of the level of product/services risk. The FI should use the same basic process described above under customer risk to determine its products and services risk.

The following table provides an example of an inherent risk rating for products and services:

Level of inherent risk regarding customers	Potential exposure to sanctions risk	Suggested assigned value
High	High – Indicates that a large portion of the FI's products and services are in the high-risk category.	5
Medium-High	Somewhat higher than moderate – Indicates that a slightly higher than a moderate portion of the FI's products and services are in the high-risk category.	4
Medium	Moderate – Indicates that a moderate portion of the FI's products and services are in the high-risk category.	3
Medium-Low	Less than moderate – Indicates a that a less than moderate portion of the FI's products and services are in the high-risk category.	2
Low	Negligible – Indicates that only a small portion of the FI's products and services are in the high-risk category.	1

To illustrate how this would work in practice, assume that an FI offers 10 products and services, having the following risk scores:

- 1 at risk level 1
- 2 at risk level 2
- 5 at risk level 3
- 1 at risk level 4
- 1 at risk level 5

For each of these levels, the FI would multiply the risk level by the number of products and services in that category:

- 1 at risk level 1 = 1
- 2 at risk level 2 = 4
- 5 at risk level 3 = 15
- 1 at risk level 4 = 4
- 1 at risk level 5 = 5

  TOTAL 29

The overall total (29) would be divided by the total number of products and services (10). The resulting risk score for this element would be 2.9, which would be rounded to the nearest whole number (3), indicating a medium risk level for products and services risk.

Delivery Channel Risk

A delivery channel is a chain of processes or intermediaries through which a product or service passes until it reaches the final buyer or the end customer/consumer. Traditionally, most financial services were delivered on a face-to-face basis, through meetings with customers at the FI's place of business, or occasionally at the customer's home or place of business. This has changed in the modern environment, with the ability to provide services remotely via the internet or through third-party intermediaries.

Delivery channel risk is closely related to customer risk. Some delivery channels/servicing methods can increase sanctions risk by making it more difficult for FIs to truly know or understand the identity and activities of their customers. Consequently, FIs must assess whether, and to what extent, their methods of customer intake or servicing, such as non-face-

to-face relationships or the involvement of third-party intermediaries could increase their inherent sanctions risk.

These non-traditional delivery methods do not always lead to an increase in the inherent sanctions risk (such as where a customer is known to the FI but undertakes much of its business activity on a non-face-to-face basis). However, unregulated customers, or those that are not well known to the FI, are much more likely to present a higher level of inherent risk.

In order to assess its delivery method risk, an FI should ask the following questions:

- Does the method of delivery used in the FI's business provide for, or encourage, anonymity?
- Does the FI's method of delivery depend on intermediaries?
- Does the method of delivery remove or minimize face-to-face contact with customers?
- Does the FI's business use a method of delivery targeted to offshore customers?
- Can a third party use this method of delivery?

FIs can apply the same basic process as described for customer risk above to determine its delivery channel risk. The key question is the portion of the FI's customers that are face-to-face customers, relative to the total customer base. Customers who conduct business with the FI exclusively via the internet or through intermediaries would be considered high-risk customers, whereas customers who conduct business with the FI exclusively in person would be considered low-risk customers. "Hybrid" customers (who conduct both face-to-face and internet or intermediary-based transactions) generally can be classified as lower-risk customers due to the FI's ability to meet them in person, although the volume of remote business of these customers, relative to the overall volume of their business, should be taken into account. Customers that are based in foreign jurisdictions, particularly those jurisdictions that are considered high-risk, are also more likely to pose a higher delivery channel risk, since they are more likely to conduct their business with the FI remotely rather than in person.

The following tables provide suggested numerical values for each sub-category of delivery channel risk.

Level of inherent delivery channel risk: Internet vs. face-to-face customers	**Potential exposure to sanctions risk**	**Suggested assigned value**
High	High – Indicates that the FI provides services exclusively via the internet.	5
Medium-High	Somewhat higher than moderate – Indicates that the FI provides services mainly via the internet, but has some face-to-face customers.	4
Medium	Moderate – Indicates that the FI provides a mixture of internet services and services to face-to-face customers.	3
Medium-Low	Less than moderate – Indicates that the FI provides services to mainly on a face-to-face basis, but conducts some business via the internet.	2
Low	Negligible –Indicates that the FI does not provide services via the internet.	1

Level of inherent delivery channel risk: Reliance on intermediaries	Potential exposure to sanctions risk	Suggested assigned value
High	High – Indicates that the FI relies exclusively on intermediaries to conduct CDD procedures, or that all or nearly all of its business with customers is conducted through intermediaries.	5
Medium-High	Somewhat higher than moderate – Indicates that the FI relies mainly on intermediaries to conduct CDD procedures, or that much of its business with customers is conducted through intermediaries.	4
Medium	Moderate – Indicates that the FI relies on intermediaries to conduct some CDD procedures, or that some of its business with customers is conducted through intermediaries.	3
Medium-Low	Less than moderate – Indicates that the FI conducts most of its CDD procedures itself, but relies on intermediaries to conduct some CDD procedures, or that only a small amount of its business with customers is conducted through intermediaries.	2
Low	Negligible –Indicates that the FI does not utilize intermediaries.	1

Level of inherent delivery channel risk: Foreign customers	Potential exposure to sanctions risk	Suggested assigned value
High	High – Indicates that the FI provides services to customers in more than 5 high-risk jurisdictions.	5
Medium-High	Somewhat higher than moderate – Indicates that the FI provides services to customers in 4 or 5 high-risk jurisdictions.	4
Medium	Moderate – Indicates that the FI provides services to customers in 2 or 3 high-risk jurisdictions.	3
Medium-Low	Less than moderate – Indicates that the FI provides services to customers in 1 high-risk jurisdiction.	2
Low	Negligible –Indicates that the FI does not provide services to customers in any high-risk jurisdictions.	1

Determining the Overall Inherent Risk Level

Once an FI has completed the above steps, it is in a position to determine its overall inherent sanctions risk. FIs often adopt quantity-related definitions and assign uniform values for each volume level to ensure more consistent measurement of its risk exposure. Sample definitions and point values for a sanctions risk assessment are provided below. The FI should calculate the simple average of the individual factors listed above, rounded to the nearest whole number, and make a determination based on the sample definitions and point values provided below.

Level of inherent risk	Potential exposure to sanctions risk	Suggested assigned value
High	High – Indicates that a large portion of the FI's activities or customer base involve high-risk customers, transactions, activities, products/services, or geographic locations.	5
Medium-High	Somewhat higher than moderate – Indicates that a somewhat higher than moderate portion (but not a large portion) of the FI's activities or customer base involve high-risk customers, transactions, activities, products/services, or geographic locations.	4
Medium	Moderate – Indicates that a moderate portion of the FI's activities or customer base	3

	involve high-risk customers, transactions, activities, products/services, or geographic locations.	
Medium-Low	Less than moderate – Indicates a that a less than moderate portion (but not a small portion) of the FI's activities or customer base involve high-risk customers, transactions, activities, products/services, or geographic locations.	2
Low	Negligible – Indicates that only a small portion of the FI's activities or customer base involve high-risk customers, transactions, activities, products/services, or geographic locations.	1

III. Controls

Once the FI has determined its inherent risk, it should proceed to analyse candidly the quality of the controls it has put in place to mitigate each category of inherent risk. This second step consists of:

(1) evaluating the contents of the control measures (i.e., the written policies and procedures) to ensure that they contain all of the necessary elements of an effective control measure); and

(2) evaluating the actual implementation of those measures (i.e., how closely the policies and procedures are followed in practice). One good indicator of this is the number of deficiencies uncovered during a reasonable look-back period (generally 12 to 24 months) by the FI's compliance function, its internal audit function, external auditors or supervisory authorities. This aspect of the evaluation should also include the promptness with which corrective action is taken when it is needed.

Depending on the effectiveness of those controls, the FI can *reduce its inherent risk* by applying the control factors to its inherent risk. Section 3.3 above identified typical internal control elements that can help an FI to mitigate its inherent risk. The following sections provide examples of how an FI might analyse its controls in each of those categories. Specific definitions and point values are assigned for each level of a control measure. The FI can assign a qualitative score depending on the contents of the control measure (point (1) above) and how well it is actually applied in practice (point (2) above).

The suggested value determines the amount by which inherent risk can be reduced. Thus, for example, an assigned value of 0.10 (i.e., 10%) would result in a reduction of 90% in the level of inherent risk. A value amount should be assigned for *each* control measure; the simple numerical average of those calculations should then be used to determine the amount by which inherent risk can be reduced (see the "Overall Conclusion Regarding Controls" table below).

Strength of control	**Suggested assigned value**
Strong	0.10 – 0.30 (70% to 90% risk reduction)
Moderate-Strong	0.30 - 0.50 (50% to 70% risk reduction)

Moderate	0.50 – 0.70 (30% to 50% risk reduction)
Moderate-Weak	0.70 – 0.90 (10% to 30% risk reduction)
Weak	0.90 - 1.00 (0 to 10% risk reduction)

It is important to note that these determinations cannot be made mechanically. Very often, when evaluating a particular control measure, either the content of the measure or its implementation (or both) will not fit neatly into the given "Description" column. It is not unusual for a control situation to "straddle" between two descriptions, containing some elements of each one. In these cases, the FI will need to closely and candidly analyse the characteristics of the control measure and make a good faith assessment of which "Description" category most closely fits those characteristics. The same principle applies to assigning the qualitative value to a control measure. The "suggested assigned value" column provides a range of values, so that the FI can assign a value that most closely corresponds to the characteristics of the control measure under consideration.

The control measures, descriptions of the different levels of control strength, and suggested values are provided below.

Written SCP

Section 3.1 of this Guideline emphasizes the importance of board and management commitment to sanctions compliance, with one of the key factors being a written SCP. The quality of that SCP reveals a great deal about the quality of an FI's sanctions program. An FI can make a judgment about the quality of its SCP from the following table:

Strength of control	Level of impact	Suggested assigned value
Strong	The FI has a formal written SCP. The policy contains clear statements of the responsibilities of the management and staff, and the sanctions compliance officer. Management reviews and updates the policy at least annually and ensures that any necessary adjustments are made, and consistently ensures that corrective action is taken when breaches are discovered. The policy is followed closely. Deviations (if any) are extremely rare, always minor, and promptly corrected.	0.10 – 0.30 (70% to 90% risk reduction)
Moderate-Strong	The FI has a formal written SCP. The policy contains clear statements of the responsibilities of management, staff, and the sanctions compliance officer. Management reviews and updates the policy at least annually and ensures that any necessary adjustments are made, and consistently ensures that corrective action is taken when breaches are discovered. The policy is nearly always followed. Deviations are minor and	0.30 - 0.50 (50% to 70% risk reduction)

	promptly corrected. There may be some minor shortcomings in the SCP, which can easily be remedied in the normal course of business.	
Moderate	The FI has a formal written SCP. The policy addresses most of the responsibilities management, staff and the sanctions compliance officer. Management occasionally reviews and updates the policy and usually ensures that any necessary adjustments are made, and usually ensures that corrective action is taken when breaches are discovered. The policy is usually followed. There are occasional deviations, which are usually corrected, but corrective action is not always as prompt as that found in the "strong" or "moderate-strong" categories.	0.50 – 0.70 (30% to 50% risk reduction)
Moderate-Weak	The FI has a formal written SCP, but the policy contains only general statements on the responsibilities of management, staff and the sanctions compliance officer. Management occasionally reviews the policy, but rarely makes adjustments. There is general lack of implementation. There are substantial deviations and corrective action is taken slowly, if at all.	0.70 – 0.90 (10% to 30% risk reduction)
Weak	The firm does not have a formal written SCP, or the policy lacks so much basic information that it is essentially meaningless. If there is a policy, there is little or no effort at implementation. There are many deviations and corrective action is rarely or never undertaken.	0.90 - 1.00 (0 to 10% risk reduction)

Customer Due Diligence and DPE Screening

Section 3.3 of this Guideline outlined the characteristics of an effective CDD and screening program. In evaluating the quality of its CDD and screening controls, an FI's board of directors should ask the following questions, and include explanatory comments if necessary:

Do the CDD policies and procedures require adherence to all the legal and regulatory requirements?	☐ Yes ☐ No
Do the CDD policies and procedures clearly indicate which customer types the FI is permitted to accept and retain?	☐ Yes ☐ No
Do the CDD policies and procedures ensure that CDD approval happens before the customer can start using a product or transacting with/through the FI?	☐ Yes ☐ No
Do the CDD policies and procedures provide clear guidance to identify beneficial owners and controlling persons (legal or natural) of customers or potential customers?	☐ Yes ☐ No
Do the CDD policies and procedures require EDD to identify any potential DPEs who are or are seeking to become customers of the FI?	☐ Yes ☐ No
Do the CDD policies and procedures provide a clearly defined EDD process with clear guidance on additional information required?	☐ Yes ☐ No
Does the FI maintain a current list of all its correspondent banking clients?	☐ Yes ☐ No
Has the FI's correspondent banking portfolio been risk-rated using an approved risk assessment methodology?	☐ Yes ☐ No
Do the CDD policies and procedures provide clear criteria to identify customers/customers that can be classified as high risks?	☐ Yes ☐ No
Does the FI conduct name screening to identify DPEs?	☐ Yes ☐ No
Does the name screening system accurately capture DPEs?	☐ Yes ☐ No

Does the name screening system effectively handle name variations?	☐ Yes ☐ No
Do the policies and procedures provide an effective means to detect false positives?	☐ Yes ☐ No
Does the FI conduct transaction screening?	☐ Yes ☐ No
Does the system effectively capture transactions that should not be carried out?	☐ Yes ☐ No
Does the FI's CDD/screening process ensure an audit trial of decisions on customer acceptance, including dates, name of the approving staff member, and full records of any rejections and reasons for rejection?	☐ Yes ☐ No
Do the policies and procedures provide an effective process to resolve discrepancies customer identification and verification?	☐ Yes ☐ No

Based on the answers to the above questions, the board of directors can use the following suggested table to evaluate the effectiveness of its CDD/screening controls:

Strength of control	Description	Suggested assigned value
Strong	The FI has an effective CDD/sanctions program. Written policies, procedures and processes are in place to identify customers and collect reliable information about their business activities, including identifying beneficial owners (BOs) of legal entity and legal arrangement customers and to identify DPEs. The policies, procedures and processes address all essential points and are consistently followed. Screening procedures consistently capture DPEs. Deviations, if any, are extremely rare, always minor and promptly corrected when discovered.	0.10 – 0.30 (70% to 90% risk reduction)
Moderate-Strong	The FI has an effective CDD/sanctions program. Written policies, procedures and processes are in place to identify customers and collect reliable information about their business activities, including identifying BOs of legal entity and legal arrangement customers and to identify DPEs. Screening procedures always or almost always capture DPEs. The policies, procedures and processes address all or nearly all essential points and are always or nearly always followed. Deviations are rare, minor and promptly corrected when discovered. There may be some minor shortcomings in the program, which can easily be remedied in the normal course of business.	0.30 - 0.50 (50% to 70% risk reduction)
Moderate	The FI has a written CDD/sanctions program. Written policies, procedures and processes are in place to identify customers and collect reliable information about their business activities, including identifying BOs of legal entity and legal arrangement customers, and to identify DPEs. The policies, procedures and processes address most of the essential points and are usually followed, but there are some deviations that occasionally result in some high-risk customers being missed, or BOs or DPEs not being identified. Deviations are usually corrected within a reasonable time when discovered, but corrective action is not always as prompt as is the case in the strong or moderate-strong category.	0.50 – 0.70 (30% to 50% risk reduction)
Moderate-Weak	The FI has a CDD/sanctions program that addresses only some of the necessary points and is not consistently followed. The policies and procedures may consist only of general informal communications rather than a comprehensive document. There are significant deviations that often result in high-risk customers or BOs being missed and/or DPEs not being identified. Corrective action to address deviations is undertaken sporadically or not at all, and there is little or no effort by the board of directors and management to ensure improvement.	0.70 – 0.90 (10% to 30% risk reduction)
Weak	There are no formal CDD/sanctions policies and procedures, or the policies and procedures exist only "on paper" and lack many essential points. There is a general lack of compliance. The board of directors and management rarely review the policies and rarely make adjustments.	0.90 - 1.00 (0 to 10% risk reduction)

	There are many deviations and corrective action is rare or non-existent.	

Sanctions Compliance Function

Section 3.3 of this Guideline outlined the characteristics of an effective program for ensuring an effective sanctions compliance function. In evaluating the quality of its sanctions compliance function, an FI's board of directors should ask the following questions, and include explanatory comments if necessary:

Has the board of directors has designated a sanctions compliance officer (SCO)?		☐ Yes ☐ No
	If "yes":	
	Does the FI have a formal document (such as a charter or terms of reference) that clearly sets out the duties and responsibilities of the SCO?	☐ Yes ☐ No
	Does the SCO have unrestricted access to the board of directors?	☐ Yes ☐ No
	Does the SCO have the necessary background and qualifications (education, experience) to effectively execute all of his/her duties?	☐ Yes ☐ No
	Does the FI have a policy that prohibits employing people with conflicts of interest or a record of fraudulent crimes or other similar criminal activities?	☐ Yes ☐ No
	Does the SCO have the necessary authority to effectively execute all of his/her duties?	☐ Yes ☐ No
	Does the SCO have the necessary resources (financial, material, technological, etc.) to effectively execute all of his/her duties?	☐ Yes ☐ No
	Is the sanctions compliance function sufficiently staffed for the FI's overall risk level (based on products, services, customers, and geographic locations), size, and sanctions compliance needs?	☐ Yes ☐ No
	Does the SCO /staff have adequate time to execute all of their duties?	☐ Yes ☐ No

Based on the answers to the above questions, the board of directors can use the following suggested table to evaluate its sanctions compliance function:

Strength of control	Description	Suggested assigned value
Strong	The FI has a written charter or terms of reference that clearly sets out the responsibilities and authorities of the sanctions compliance officer (SCO). The SCO has unrestricted access to the board of directors. The SCO has the necessary background and qualifications (education,	0.10 – 0.30 (70% to 90% risk reduction)

	experience) to effectively execute all of his/her duties and is thoroughly familiar with the UNFSA, AML/CFT Act, U.N. Security Council resolutions regarding sanctions and recommendations of international standard-setting bodies regarding sanctions compliance. The SCO diligently maintains his/her knowledge and passes new developments on to the FI's management, board of directors and staff who deal with sanctions matters in their work. The compliance function is sufficiently staffed and has the necessary resources (financial, material, technological) to perform its duties. If the sanctions compliance function contains staff members in addition to the SCO, the staff members clearly have the necessary background, training and experience to perform their duties. The FI's management and board of directors have consistently demonstrated responsiveness to audit findings and consistently take prompt corrective action when necessary.	
Moderate-Strong	The FI has a written charter or terms of reference that clearly sets out the responsibilities and authorities of the SCO. The SCO has unrestricted access to the board of directors. The SCO has the necessary background and qualifications (education, experience) to effectively execute all of his/her duties and is thoroughly familiar with the UNFSA, AML/CFT Act, U.N. Security Council resolutions regarding sanctions and recommendations of international standard-setting bodies regarding sanctions compliance. The SCO diligently maintains his/her knowledge and passes new developments on to the FI's management, board of directors and staff who deal with sanctions matters in their work. The compliance function is adequately staffed and has the necessary resources (financial, material, technological) to perform its duties. If the sanctions compliance function contains staff members in addition to the SCO, the staff members have adequate background, training and experience to perform their duties. The FI's management and board of directors have consistently demonstrated responsiveness to matters identified by the SCO as requiring attention and always or nearly always take prompt corrective action when necessary. There may be some minor shortcomings in the sanction compliance program, but these can easily be remedied in the normal course of business.	0.30 - 0.50 (50% to 70% risk reduction)
Moderate	The FI has a written charter or terms of reference that sets out the responsibilities and authorities of the SCO, although some elements may need clarification or strengthening. The SCO has access to the board of directors. The SCO has the adequate background and qualifications (education, experience) to effectively execute all of his/her duties and is generally familiar with the UNFSA, AML/CFT Act, U.N. Security Council resolutions regarding sanctions and recommendations of international standard-setting bodies regarding sanctions compliance. The SCO maintains his/her knowledge and passes new developments on to the FI's management, board of directors and staff who deal with sanctions matters in their work. The compliance function is adequately staffed and has the most of the necessary resources (financial, material, technological) to perform its duties. If the sanctions compliance function contains staff members in addition to the SCO, the staff members have the general background, training and experience to perform their duties. The FI's management and board of directors have usually demonstrated responsiveness to matters identified by the SCO as requiring attention and usually take corrective action when necessary, although such corrective action is sometimes delayed.	0.50 – 0.70 (30% to 50% risk reduction)
Moderate-Weak	The FI has a written charter or terms of reference that generally sets out the responsibilities and authorities of the SCO, but the document is rather superficial and is missing some key elements. The SCO's access	0.70 – 0.90 (10% to 30%

	to the board of directors is sometimes questionable. The SCO has minimal background and qualifications (education, experience) to effectively execute all of his/her duties and is only basically familiar with the UNFSA, AML/CFT Act, U.N. Security Council resolutions regarding sanctions and recommendations of international standard-setting bodies regarding sanctions compliance. The SCO does not consistently maintain his/her knowledge or pass new developments on to the FI's management, board of directors and staff who deal with sanctions matters in their work. The compliance function is not sufficiently staffed and does not have the necessary resources (financial, material, technological) to perform its duties. If the sanctions compliance function contains staff members in addition to the SCO, the staff members do not have the necessary background, training and experience to perform their duties effectively. The FI's management and board of directors have not demonstrated responsiveness to matters raised by the SCO as requiring attention and rarely take corrective action in response to deviations from legal or regulatory requirements or internal FI policies and procedures regarding sanctions compliance.	risk reduction)
Weak	The FI does not have a formal sanctions compliance program, or has a program that appears to exist only "on paper" and is largely ignored. There is a general lack of compliance with legal/regulatory requirements and internal FI policies and procedures. The SCO does not have the necessary background or qualifications (education, experience) to effectively execute all of his/her duties and is unfamiliar with the UNFSA, AML/CFT Act, U.N. Security Council resolutions regarding sanctions and recommendations of international standard-setting bodies regarding sanctions compliance. The SCO does not maintain his/her knowledge or pass new developments on to the FI's management, board of directors and staff who deal with sanctions matters in their work. The compliance function is not sufficiently staffed and does not have the necessary resources (financial, material, technological) to perform its duties. If the sanctions compliance function contains staff members in addition to the SCO, the staff members do not have the necessary background, training and experience to perform their duties. The FI's management and board of directors have not demonstrated responsiveness to sanctions compliance matters. FIs in this category tend to regard sanctions compliance as more of a nuisance that interferes with the pursuit of revenue rather than as an important aspect of their work.	0.90 - 1.00 (0 to 10% risk reduction)

Independent Testing/Auditing

Section 3.4 of this Guideline described the characteristics of an effective independent testing program for sanctions compliance. In evaluating the quality of its internal audit/independent testing function, an FI's board of directors should ask the following questions, and include explanatory comments if necessary:

Is the independent audit function in fact independent (i.e., performed by a person or persons not involved with designing or implementing the FI's sanctions compliance function)?	☐ Yes ☐ No
Does the independent audit function report directly to the board of directors or to a designated board committee consisting primarily or entirely of independent directors (preferably the audit committee)?	☐ Yes ☐ No

Does the FI have a formal document (such as a charter or terms of reference) that clearly sets out the duties and responsibilities of the internal audit function regarding sanctions compliance?	☐ Yes ☐ No
If the internal audit function is outsourced, are there written procedures governing the relationship between the audit provider and the board of directors?	☐ Yes ☐ No
Does the internal audit/testing process address:	
• The overall adequacy and effectiveness of the sanctions compliance program, including policies, procedures, and processes?	☐ Yes ☐ No
• The adequacy of the FI's sanctions risk assessment?	☐ Yes ☐ No
• Reporting and recordkeeping requirements related to sanctions compliance?	☐ Yes ☐ No
• CDD and screening policies, procedures, and processes and whether they comply with the UNFSA, related regulations, and the FI's internal requirements?	☐ Yes ☐ No
• An evaluation of the system's ability to identify BOs and actual controlling persons or entities of customers (including potential customers)?	☐ Yes ☐ No
• Personnel adherence to the FI's policies, procedures, and processes regarding sanctions?	☐ Yes ☐ No
• Appropriate transaction testing, with particular emphasis on higher-risk operations (products, services, customers, and geographic locations)?	☐ Yes ☐ No
• The adequacy of the FI's training on sanctions matters, including comprehensiveness, accuracy of materials, the training schedule, and attendance tracking?	☐ Yes ☐ No
• The appropriateness and accuracy of Management Information System (MIS) for screening customers and transactions given the FI's risk profile?	☐ Yes ☐ No
• Tracking of previously identified issues and deficiencies, and verification that they have been corrected by management?	☐ Yes ☐ No
Are audit reports clear, thorough, well-written so as to provide useful information to the board of directors as to the overall effectiveness of the FI's sanctions compliance program?	☐ Yes ☐ No

Have the FI's management and board of directors demonstrated responsiveness to audit findings (i.e., taking action to correct any identified deficiencies in the sanctions compliance program)?	☐ Yes ☐ No

Based on the answers to the above questions, the board of directors can use the following suggested table to rate its internal audit/independent testing program regarding sanctions compliance:

Strength of control	Description	Suggested assigned value
Strong	The FI has a written charter or terms of reference that clearly sets out the responsibilities and authorities of the independent audit function. The independent audit function is in fact independent and reports directly to the board of directors or to a designated board committee consisting primarily or entirely of independent directors (preferably the audit committee). The internal audit/testing process addresses the content of the FI's sanctions policies and procedures and their overall implementation; the FI's sanctions risk assessment for reasonableness given the FI's risk profile (products, services, customers, entities, and geographic locations); the effectiveness of the FI's customer and transaction screening systems; the board's and management's efforts to remedy any violations and deficiencies noted in previous audits and BPNG inspections, including progress in addressing outstanding corrective actions required by the BPNG/FASU, if applicable; the FI's staff training for adequacy, accuracy, and completeness; an assessment of the reporting process to the FASU, including a review of filed or prepared reports to determine their accuracy, timeliness, and completeness. Internal audit reports consistently reflect that independent testing is thorough and comprehensive and contain specific and detailed conclusions and recommendations for the board of directors. The FI's management and board of directors have consistently demonstrated responsiveness to audit findings and consistently take prompt corrective action when necessary.	0.10 – 0.30 (70% to 90% risk reduction)
Moderate-Strong	The FI has a written charter or terms of reference that clearly sets out the responsibilities and authorities of the independent audit function. The independent audit function is in fact independent and reports directly to the board of directors or to a designated board committee consisting primarily or entirely of independent directors (preferably the audit committee). The internal audit/testing process addresses all or nearly all of the items listed under the "Strong" category. Internal audit reports reflect that independent testing is nearly always thorough and comprehensive, and reports always or nearly always contain specific and detailed conclusions and recommendations for the supervisory board. The FI's management and board have generally demonstrated responsiveness to audit findings and always or nearly always take prompt corrective action when necessary.	0.30 - 0.50 (50% to 70% risk reduction)
Moderate	The FI has a written charter or terms of reference that sets out the responsibilities and authorities of the independent audit function. The independent audit function is in fact independent and reports directly to the board of directors or to a designated board committee consisting primarily or entirely of independent directors (preferably the audit committee). The internal audit/testing process addresses most of the items listed under the "Strong" category. Internal audit reports reflect that independent testing is generally adequate, but some areas may not be comprehensively addressed or thoroughly tested, leading to the	0.50 – 0.70 (30% to 50% risk reduction)

	possibility of some operational shortcomings being missed. Reports usually contain useful conclusions and recommendations for the board, but because of some gaps in the testing, reports may not always address all critical areas. The FI's management and board have generally demonstrated responsiveness to audit findings and usually take corrective action to address deficiencies, although corrective action is sometimes delayed.	
Moderate-Weak	Independent testing is in place, but significant areas are not comprehensively addressed or thoroughly tested, leading to the possibility of significant operational shortcomings being missed. Reports may contain some useful information for the board, but because of gaps in the composition of the audit function or the testing process (or both), the reports do not address many critical areas and the board is not in a position to know whether the SCP is functioning effectively. The FI's management and board have not demonstrated responsiveness to audit findings and rarely take corrective action to address deficiencies.	0.70 – 0.90 (10% to 30% risk reduction)
Weak	Independent testing is not conducted, or appears to exist only "on paper." Many significant areas are not comprehensively addressed or thoroughly tested. Audit reports rarely contain useful conclusions and recommendations for the board, and because of significant gaps in the testing, reports do not address many critical areas. The FI's management and board have not demonstrated responsiveness to audit findings and rarely take corrective action to address deficiencies.	0.90 - 1.00 (0 to 10% risk reduction)

Recordkeeping and Reporting to FASU

Section 3.3 of this Guideline describes the elements of an effective recordkeeping and reporting policy regarding sanctions compliance. In evaluating the quality of its recordkeeping and reporting program, an FI's board of directors should ask the following questions, and include explanatory comments if necessary:

Does the FI have written policies and procedures concerning record keeping and reporting regarding sanctions compliance?	☐ Yes ☐ No
Is information and documentation regarding sanctions compliance readily accessible and retrievable by persons who have need of access?	☐ Yes ☐ No
Does the documentation demonstrate that requirements of the UNFSA and related regulations, including FASU reporting obligations have been met?	☐ Yes ☐ No
Are records easily accessible by those with a need of access in their work?	☐ Yes ☐ No
Does the policy include means to ensure that records are physically secured so as to prevent unauthorized access and misuse?	☐ Yes ☐ No
Do retained records include information that the FI uses to screen customers and how it resolved any discrepancies regarding customer identification or DPE status?	☐ Yes ☐ No

Does the documentation include information about activities, patterns of behaviour and other situations that may indicate attempted sanctions evasion?	☐ Yes ☐ No
Are records well-organized and accurate?	☐ Yes ☐ No
Are reports required to be submitted to FASU consistently accurate and consistently filed on time?	☐ Yes ☐ No

Based on the answers to the above questions, the board of directors can use the following suggested table to rate its recordkeeping and reporting controls regarding sanctions compliance:

Strength of control	Description	Suggested assigned value
Strong	The FI has a written policy on recordkeeping and reporting regarding sanctions compliance. The policy is consistently followed. Deviations, if any, are extremely rare, always minor, and promptly corrected when discovered. Required reports to FASU are consistently submitted on time and are consistently accurate. Errors, if any, are extremely rare, always minor and are promptly corrected when discovered.	0.10 – 0.30 (70% to 90% risk reduction)
Moderate-Strong	The FI has a written policy on recordkeeping and reporting regarding sanctions compliance. The policy is always or almost always followed. Deviations are rare, minor and promptly corrected when discovered. Required reports to FASU are always or almost always submitted on time and are always or almost always accurate. Errors are rare, minor and promptly corrected when discovered	0.30 - 0.50 (50% to 70% risk reduction)
Moderate	The FI has a written policy on recordkeeping and reporting regarding sanctions compliance, but there are some shortcomings that go beyond minor occurrences. Deviations are usually corrected within a reasonable time when discovered, but corrective action is not always as prompt as in the "strong" or "moderate-strong" categories. Required reports to FASU are usually submitted on time and are usually accurate. Errors are usually corrected when discovered.	0.50 – 0.70 (30% to 50% risk reduction)
Moderate-Weak	The FI has a superficial written policy on recordkeeping and reporting regarding sanctions compliance, or the policy consists of informal advice (ad-hoc email communications, etc.) The policy is not consistently followed, and records are often inaccurate or poorly organized. Corrective action is not consistently taken when deficiencies are discovered.	0.70 – 0.90 (10% to 30% risk reduction)
Weak	There is no formal policy on recordkeeping and reporting regarding sanctions compliance, or the policy appears to exist only "on paper" and is largely ignored. Records are sloppily maintained and are often inaccurate. Corrective action is rarely or never taken when deficiencies are discovered. Required reports to FASU are rarely submitted on time (if at all) and there are many inaccuracies in the reports. Errors are rarely or never corrected when discovered.	0.90 - 1.00 (0 to 10% risk reduction)

Training

Section 3.5 of this Guideline describes the elements of an effective training program for sanctions compliance. In evaluating the quality of its sanctions training program, an FI's board of directors should ask the following questions, and include explanatory comments if necessary:

Do senior management and the board of directors place a high degree of importance on ongoing education and training to ensure sanctions compliance?	☐ Yes ☐ No
Do senior management and the board of directors provide sufficient resources for an effective training program?	☐ Yes ☐ No
Does the training program consider all sanctions risk categories that are relevant to the FI's work?	☐ Yes ☐ No
Do training materials cover the relevant laws, regulations and the FI's sanctions policies, procedures, and processes (including changes and updates)?	☐ Yes ☐ No
Do training materials cover different forms of attempted sanctions evasion that are likely to be encountered in the FI's business?	☐ Yes ☐ No
Does the training program adequately address employee accountability for ensuring sanctions compliance?	☐ Yes ☐ No
Do personnel from all applicable areas of the FI receive training?	☐ Yes ☐ No
Are the persons providing training thoroughly knowledgeable about relevant laws, regulations, and the FI's internal policies, procedures and processes, and do they keep up with changes and updates in these areas?	☐ Yes ☐ No
Does the FI keep records of attendance at training sessions?	☐ Yes ☐ No
Do training materials cover penalties for noncompliance with internal policies and regulatory requirements?	☐ Yes ☐ No
Is knowledge checked based on training provided?	☐ Yes ☐ No
Is effective remedial action is taken in cases of non-attendance or demonstrated knowledge deficiencies?	☐ Yes ☐ No

Based on the answers to the above questions, the board of directors can use the following suggested table to rate its training program regarding sanctions compliance:

Strength of control	**Description**	**Suggested assigned value range**
Strong	The FI has a formal written sanctions training program. Training is comprehensive, covers all applicable legal and regulatory requirements, and covers all sanctions risks to which the FI is exposed. Training is provided to all personnel who need sanctions knowledge to perform	0.10 – 0.30 (70% to 90% risk reduction)

	their functions. Training materials are thorough, comprehensive, and updated as necessary. Training is provided to all relevant personnel within a reasonable time after onboarding and refresher training is provided periodically. Attendance is tracked and knowledge is checked effectively, and remedial action is taken in cases of non-attendance or demonstrated knowledge deficiencies. The persons delivering the training are thoroughly knowledgeable about sanctions compliance and risks, and keep informed about new developments. Sufficient resources are provided to ensure effective training.	
Moderate-Strong	The FI has a formal written AML/CFT training program. Training is comprehensive, covers all or nearly all applicable legal and regulatory requirements, and covers all or nearly all sanctions risks to which the FI is exposed. Training is provided to all personnel who need sanctions knowledge to perform their functions. Training materials are generally thorough, comprehensive, and updated as necessary. Training is provided to all relevant personnel within a reasonable time after onboarding and refresher training is provided periodically. Attendance is tracked and knowledge is checked effectively, and remedial action is nearly always taken in cases of non-attendance or demonstrated knowledge deficiencies. The persons delivering the training are adequately knowledgeable about sanctions compliance and risks, and keep informed about new developments. Sufficient resources are provided to ensure compliance. There may be some minor weaknesses in the program, which can easily be corrected in the normal course of business.	0.30 - 0.50 (50% to 70% risk reduction)
Moderate	The FI has a formal written sanctions training program. Training is generally adequate, covers most of the applicable legal and regulatory requirements, and covers most sanctions risks to which the FI is exposed. Training is usually provided to personnel who need sanctions knowledge to perform their functions, but there may be occasional gaps. Training materials are generally adequate, and updated as necessary, although updating may sometimes be delayed. Training is usually provided to all relevant personnel within a reasonable time after onboarding and refresher training is provided occasionally. Attendance is tracked and knowledge is usually checked. Remedial action is usually taken within a reasonable time in cases of non-attendance or demonstrated knowledge deficiencies, although remedial action is not always as prompt as is the case in the "strong" or "moderate-strong" categories. The persons delivering the training are generally knowledgeable about sanctions compliance and risks, and usually keep informed about new developments, though there are some occasional gaps. Training resources are generally adequate but could be improved.	0.50 – 0.70 (30% to 50% risk reduction)
Moderate-Weak	The FI has a formal written sanctions training program, but the program is lacking in several key areas. Training is not comprehensive, covers only some of the applicable legal and regulatory requirements, and does not cover all of the sanctions risks to which the FI is exposed. Training is provided to some, but not all, personnel who need sanctions knowledge to perform their functions. Training materials are superficial and not consistently updated. Training is not always provided to all relevant personnel within a reasonable time after onboarding and refresher training is rarely or never provided. Attendance is not tracked, knowledge is not checked, and remedial action is rarely or never taken in cases of non-attendance or demonstrated knowledge deficiencies. The persons delivering the training are only marginally knowledgeable about AML/CFT compliance and ML/TF risks, and do not keep informed about new developments. Sufficient resources are not provided to ensure effective training.	0.70 – 0.90 (10% to 30% risk reduction)
Weak	The FI does not have a formal AML/CFT training program, or the	0.90 - 1.00

	program exists only "on paper." Training is rarely or never conducted. Training materials are patently inadequate. Attendance is not tracked, knowledge is not checked, and remedial action is rarely or never taken in cases of non-attendance or demonstrated knowledge deficiencies. The persons delivering the training are plainly unfamiliar with sanctions compliance and risks, and do not keep informed about new developments. Sufficient resources are not provided to ensure effective training.	(0 to 10% risk reduction)

Overall Conclusion Regarding Controls

Once the FI has analysed each control area, it should calculate the numerical average of the scores for each area. The result will indicate the amount of reduction that can be applied to the inherent risk rating to arrive at the FI's residual risk.

IV. Residual Risk

Once an FI's inherent risks have been identified and mitigation techniques have been applied, the FI is in a position to determine its residual risk, and can design a comprehensive sanctions compliance program that best fits its needs. Residual risk is the risk that remains after controls have been applied to address inherent risks. In other words, residual risk can be viewed as the product of the assigned values of each inherent risk and the assigned mitigation/control factor. A basic formula is:

Inherent Risk × Control Impact = Residual Risk

To illustrate, assume that an FI assesses its inherent sanctions risk to be high (level "5"), but has very good controls, which it assesses at .20 (amounting to an 80% risk reduction). Applying the 80% risk reduction to the inherent risk level of 5 results in a residual risk of 1 (5 X .20), which is in the "medium to low" range. Similarly, an FI that assesses its inherent risk to be medium (level "3"), and has very good controls, which it assesses at .20 (amounting to an 80% risk reduction), would have a residual risk of 0.6 (3 X .20), which is in the "low" range. An example of categorization of residual risk could be:

Level	Characteristics
Low **Less than 1**	Exposure to sanctions risk is negligible. Risk has been properly addressed and controls are effective in mitigating the majority of risk in this area.
Medium-Low **1 – 1.99**	There is less than moderate exposure to sanctions risk. Risk has generally been properly addressed and controls are generally effective in mitigating the majority of ML/TF risk.
Medium **2.0 – 2.99**	There is moderate exposure to sanctions risk, or there are moderate weaknesses in the applicable control structure. Risks have generally been addressed and associated controls are moderately effective, although improvement in certain areas is necessary. Risk levels are generally mitigated by control activities and routines, although some improvement is necessary.
Medium-High **3.0 – 3.99**	There is somewhat higher than moderate exposure to sanctions risk, or substantial weaknesses in the applicable control structure. Significant risk areas may not have been assessed, controls may not be effective, or performance of control activities may be inconsistent. Risk levels are only marginally mitigated by control activities and routines.
High	Exposure to sanctions risk is high, as significant risk areas are not addressed, controls

4.0 – 5	are not comprehensive, or performance of control activities is ineffective in reducing risk.

V. Using the Risk Assessment as the Basis for Risk Controls

Once the risk assessment is complete and the FI's sanctions risk exposure is understood, the FI will be in a strong position to design a compliance program that is specifically tailored to its customer base, the nature of services it provides, and the size and complexity of its operations. This will necessarily vary depending on the nature of the FI. Some FIs have relatively simple operations and deal mainly with long-established customers; others engage in complex transactions for customers spanning multiple jurisdictions.

The board of directors and management should review the risk assessment for reasonableness in view of all of the FI's circumstances, and should consider the staffing resources and the level of training necessary to promote adherence with the board-approved policies, procedures, and processes. For those FIs that take on a higher-risk profile, the board and management should provide a more rigorous sanctions compliance program that specifically monitors and controls the higher risks that the FI has decided to accept.

VI. Updating the Risk Assessment

An effective risk assessment should not be a one-time exercise, but an ongoing process. FIs should periodically review their risk assessments to identify changes in their risk profile and make any necessary adjustments to their sanctions policies and procedures. This should apply in particular when new services are introduced, existing services are changed, relationships with higher-risk customers are established or terminated, or the FI undergoes a structural change such as merging with another FI or taking on a large number of new customers, particularly if those customers are considered high-risk, have high-risk business contacts or do business in high-risk jurisdictions. Even without these changes, it is a good business practice for FIs to periodically reassess their sanctions risk, and update their risk assessment at least annually.

VII. Consolidated Sanctions Risk Assessment

FIs that are parts of financial groups face special risks that are not present in stand-alone enterprises. As used in this Guideline, a "financial group" includes a parent company and its subsidiaries. These risks encompass a number of business areas and operations, some of which have important implications for sanctions compliance. They include:[1]

- **Contagion**: This is the risk that financial difficulties encountered by one member of a group can adversely affect other group members. This is mainly a matter of perception. News of problems in affiliated companies can cause loss of confidence among customers of an FI. In the sanctions context, if one member of a group is perceived by members of the public as facilitating TF or PF, it could negatively impact the reputation of other members of the group, which in turn can cause those other members to lose business.

  This is a particular problem for banks. News that a bank's affiliated company is involved in criminal activity can precipitate a sharp decline in depositor confidence, leading to

[1] Reference: Bank of England. 1998. *Handbooks in Central Banking: Consolidated Supervision of Banks*.

substantial rapid withdrawals of deposits, resulting in a severe liquidity deficiency. If the problem escalates, a major "run" on deposits can even spread to other banks, precipitating a banking crisis.

- **Quality of management and controlling persons:** In cases where an FI is controlled by a parent company, the managers and controllers of the parent company might exercise their control in a manner that is detrimental their subsidiary enterprises and their customers. In the AML/CFT/sanctions context, if the parent company's management fails to understand AML/CFT/sanctions compliance issues and its board does not adopt effective group-wide policies, the AML/CFT/sanctions compliance of the subsidiary institutions can be compromised.

- **Group structure and transparency:** Financial groups frequently have very complex structures, which can make the implementation of group-wide policies difficult. Lines of accountability within the group must be clearly communicated and thoroughly understood by all personnel within the group who are responsible for sanctions compliance.

Because of these risks, FIs need to apply their sanctions risk management programs to their foreign branches (if any) and majority-owned subsidiaries to the extent that applicable laws and regulations in the country where the foreign branch or majority owned subsidiaries are domiciled so permit.[2] If such laws or regulations prevent compliance with these obligations for any reason, the FI should report this to its supervisor, so that they may take such steps as it believes to be appropriate to accomplish the purpose of the UNFSA and related regulations.

FIs subjects to which this situation applies should assess their sanctions risk both individually within their own business lines and across all activities conducted by themselves, their branches and subsidiaries. Aggregating sanctions risks on a consolidated basis for larger or more complex FIs enables an FI to better identify risks and risk exposures within and across specific lines of business or product categories. Consolidated information also assists senior management and the board of directors in understanding and appropriately mitigating risks across the group.

To avoid having an outdated understanding of sanctions risk exposures, the FI should continually reassess its sanctions risks and communicate with business units, branches, and subsidiaries. The identification of a sanctions risk or deficiency in one area of business or entity within a wider group may indicate concerns elsewhere in group, which management should identify and control.

[2] FATF. 2019. Recommendation No. 26 (Regulation and supervision of FIs)

APPENDIX 2 – COMMON ISSUES REGARDING NAME SCREENING[1]

- *Variations in upper and lower cases*.

- *Identical matching*, in which the full name is matched against all the lists. This involves the ensuring the accuracy of the matching process itself, and ensuring that the data will provide a positive match against different sources.

- *Missing or additional hyphens or spaces.* These can occur when character sets are converted (for example, a non-Latin name to a Latin name). FIs should ensure that their screening system can deal with differences in punctuation, and missing components or letters.

- *Missing components/letters or truncated names* can become especially troublesome with very long last names. FIs need to be aware of any character limitations in any fields within their screening system, and what happens if that limitation is exceeded.

- *Incorrect database fields* can occur if data is entered from other systems are not divided correctly.

- *Spelling differences* in names that can be spelled in different ways (examples: "Sean" vs. "Shaun," "Shawn," or "Sian");

- *Nicknames:* (example: "Willliam," "Bill," "Will," "Billy," or "Willy").

- *Titles and Honorifics,* such as "Reverend," "Imam," "Mister," "Miss," "Lady" or "Lord." FIs should ensure that their screening system can handle these.

- *Out of order components,* such as when given names are switched with surnames.

- *Multiple languages.* FIs should ensure that their system can handle names in their native character set such as Arabic or Chinese.

- *AKAs* ("also known as"). FIs should know how their system handles these variations.

- *Initials*. FIs should know how the system handles initials rather than the full first names.

- *Similar names or phonetic similarities:* Names that may sound similar but are in fact different (example: "Jang" and "Jung").

- *Noise simulation*, where characters are added or are switched (for example, insertion of extraneous characters or when a zero is used instead of the letter O.

[1] Adapted from Alessa, Inc., *How to Test Your Sanctions and Watch List Screening Software*, *https://alessa.com/wp-content/uploads/2020/06/How-To-Test-Sanctions-Screening-Software.pdf*

- *Accents, Transliteration and Translation*: Screening names in their non-Latin native characters can be challenging for FIs that communicate in languages that use Latin characters. However, even languages that use Latin characters, like Spanish, Portuguese, Dutch, French and German, can be challenging due to some unique letters and accents. The system needs be able to deal with names with and without accents (for example, the Hispanic name Jose/José). FIs also need to decide how to handle variations such as "Joe," or "Joseph," which can be a translation of José. Non-Latin conversions are particularly complex. Some systems transliterate names, while others translate them (transliteration is the process of transferring a word from one alphabet or language into the corresponding, similar-sounding characters of another alphabet, such as from the Latin to the Cyrillic; translation informs the meaning of a word in another language).

- *Variations of Muhammed*: The name Muhammad is one of the most common first names in the world. There are at least 65 common variations of this name, and it is one of the most frequently misspelled when it comes to onboarding customers. The spelling of the name varies based on different jurisdictions, different standards across different countries and in different scripts. FIs need to be sure that the way the person spells it is the way it actually appears on file. Problems arise when there is an error in data input or how the name was entered.

- *Variations by region:* There are also many other complexities according to geographic region.

  - Some of the most complex issues revolve around marriage. In Western Europe and North America, many people assume that a person's surname is the father's last name. Also, by tradition, when a woman gets married, she adopts her husband's last name, but that tradition is changing. The situation is different in Spanish speaking Latin America; a person's last name is the father's first last name and then the mother's first last name. In most countries in Latin America, women do not change their names when they get married. The tradition is still different in Portuguese speaking countries. In Brazil, a person's surname is the mother's first last name followed by the father's first last name. Therefore, an FI will likely run into some complexities in the case of customers from Latin American countries. For example, if it has a customer who is originally from Brazil, but now has moved to Colombia, there can be some very complex issues as that person's name may now be changed.

  - In some countries (e.g., Eritrea, Ethiopia and Iceland), there are cases where a person's last name is the father's first name rather than a traditional last name.

  - In the Arab world, names may be [first name] bin [father's name] [sometimes another descriptor such as a family name or ancestral home].

  - In Japan, China and Korea, the last name appears first, although in Japan this is beginning to change to a western style in documents that appear with the Latin alphabet.

APPENDIX 3 – GUIDANCE ON BENEFICIAL OWNERSHIP

Overview

One of the most critical aspects of customer identification is knowing the *beneficial owner* (BO) of an account or of a legal entity or legal arrangement that seeks to become a customer. Section 5(1) of the AML/CFT Act defines a "beneficial owner" as a natural person who –

- has ultimate control, directly or indirectly, of a customer; or
- ultimately owns, directly or indirectly, the customer.

Thus, there are two means of determining beneficial ownership, both of which need to be taken into account:

- the "ownership" component; and
- the "control" component.

According to FASU Guidance, "control" includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, where or not having legal or equitable force and whether or not based on legal or equitable rights. This includes exercising control through the capacity to make decisions about financial and operating policies.

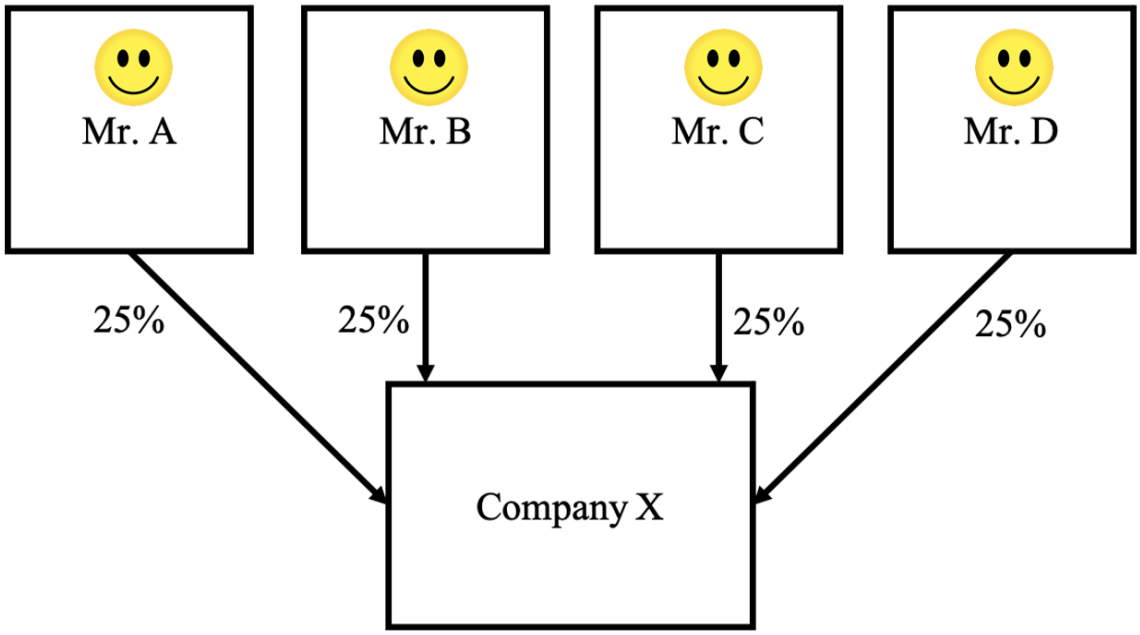
"Owns" means ownership, either directly or indirectly, of 25% or more of a person or unincorporated entity.

Both components should be examined. In other words, once the 25% numerical threshold is reached, that person should be considered a BO, regardless of whether there is also a *de facto* controlling person. However, the inquiry should not stop there. It should also be determined whether there is any person who exercises actual control, even if owning less than the requisite ownership amount of shares or voting power, and even if a BO can be identified based on share ownership. The rationale for this approach is that while in some cases the BO may appear to be clear based on the ownership structure, in fact there may be a *de facto* controlling person with little or no formal ownership. In order to be certain that all possible means of control have been addressed, this inquiry should be made.

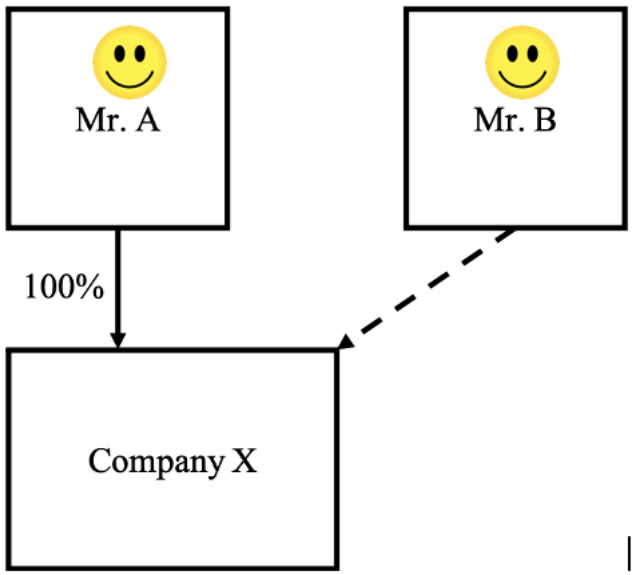
Most of the discussion below will pertain to companies. However, beneficial ownership of cooperatives, partnerships, trusts,[11] non-profit organizations and other legal persons and legal arrangements must also be kept in mind.

In the following simple example, "Mr. A," "Mr. B," "Mr. C" and "Mr. D" are all BOs of Company X, because each of them owns at least 25% of the shares of Company X.

[11] In the case of a trust, according to FATF standards, there is no numerical ownership threshold. A natural person who is a trustee, settlor, protector, and beneficiary of a trust should be considered a BO of the trust.



A person may be a BO under the "control" component while owning few or no shares. The following simple example illustrates this point:



In this example, "Mr. A" owns all of the shares, and holds all of the voting rights, of Company X. However, "Mr. B" makes all of the decisions about Company X. Both Mr. A and Mr. B would be considered BOs of Company X.

It is possible that in some circumstances the same person or persons might be identified pursuant to both the "ownership" and "control" components. For example, in the scenario presented above, if one of the legal owners is an actual controlling person, there would be 4 BOs – the 4 individuals who each own 25% of the company, one of whom would also be the

actual "control" person. However, it is also possible that in addition to the four 25% owners, there could be a different person who has no formal ownership interest, but who exercises real control of the company. In this scenario, there would be as many as 5 persons who would qualify as BOs – the four 25% shareholders, and the person who actually controls the company. This will occur most often in the case of "nominee" shareholders, but could occur in any situation of "*de facto"* or concealed beneficial ownership.

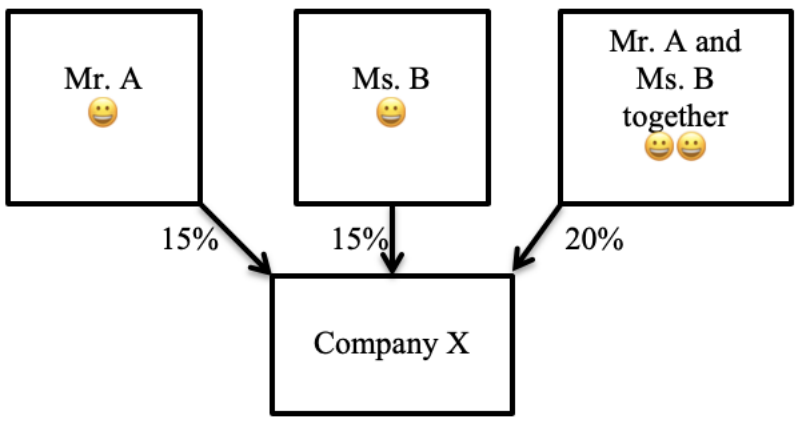
The Ownership Component

The first task is to determine who owns shares in a company. Such ownership may be direct or indirect, i.e., through one or more controlled entities, such as subsidiaries. It includes ownership that is exercised alone or jointly with one or more other persons.

Direct Ownership

Direct ownership refers to actual direct legal ownership of shares of a legal entity. In most companies, this is a fairly straightforward matter. The legal owner(s) will be the person or persons listed as shareholders on the register of members or shareholders. In simpler structures (i.e., with only one layer of ownership), these are likely to be natural or legal persons who hold their shares for themselves. Any such natural person who holds at least 25% of the issued share capital or voting rights would therefore be both the legal owner of the shares and a BO of that company.

It is important to note that where shares are owned jointly by more than one person, this must be taken into account in determining those persons' total ownership. For example, if two or more shareholders own shares jointly, they are both considered to own all of the shares, and their percentage ownership will include their joint holding and any other shareholding. A simple example follows:

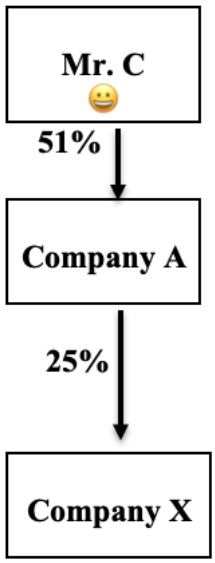


In the above example, shareholders Mr. A and Ms. B are natural persons who each own 15% of Company X in their individual capacities. In addition to their individual holdings, they jointly own 20% of the company. The shares that are owned jointly (here, 20%) are combined with the shares that each of them owns individually (here, 15% each). Mr. A and Ms. B would

thus be considered BOs of the company, as each would be the owner of his or her 15% plus the 20% held jointly with the other shareholder (total 35% each).

Indirect Ownership

Indirect ownership refers to ownership that is achieved through one or more controlled enterprises, or through a "chain of ownership." The following example illustrates this.



In the above example, "Mr. C" owns 51% of Company A, which holds 25% of Company X; Mr. C is therefore a beneficial owner of Company X.

A potential problem for FIs is that legal entities sometimes have multiple layers of ownership. Criminals frequently use this technique to conceal their beneficial ownership of legal entities. The question is how to determine 25% ownership beyond the second level where there are multiple ownership layers. For this purpose, the "**majority stake**" test should be applied.

The Majority Stake Test

The *majority stake* test entails determining whether any person holds shares in a company through one or more entities in which he or she holds a "majority stake," which entails direct or indirect ownership of 50% or more of the voting shares or capital; if so, ownership held by a shareholder is attributed *in full* to any person that holds a majority stake (whether a natural or legal person) in that shareholder.

A person holds a share indirectly if the person has a majority stake in a legal person or legal arrangement and that legal person or legal arrangement:

- holds the share in question; or
- is part of a chain of legal persons or legal arrangements:
  - each of which (other than the last) has a majority stake in the legal person or legal

arrangement immediately below it in the chain; and

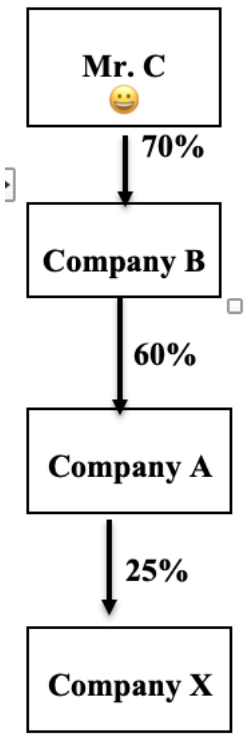
– the last of which holds the share.

A person holds a right indirectly if the person has a majority stake in a legal person or legal arrangement and that legal person or legal arrangement:

- holds that right; or
- is part of a chain of legal persons or legal arrangements:
  - each of which (other than the last) has a majority stake in the legal person or legal arrangement immediately below it in the chain; and
  - the last of which holds that right.

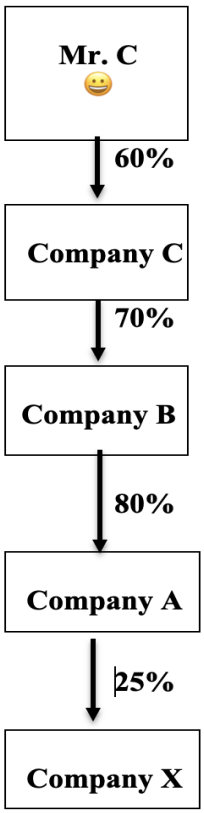
According to this definition, the majority stake test is only applicable where there is an unbroken chain of at least 50% ownership in the chain of legal persons or legal arrangements (other than the one in question). It is important to note that the real focus here is the "second" ownership layer (i.e., the entity that owns at least 50% of the 25% legal entity shareholder of the entity in question).

The following example illustrates how the majority stake test works in practice:



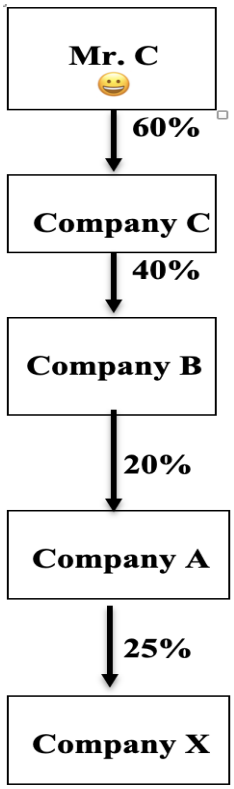
In the above example, "Mr. C" has a majority stake (70%) in Company B, which owns 60% of Company A, which holds 25% of Company X. Mr. C would be considered a BO of Company X.

This same principle applies regardless of how many layers there may be in an ownership chain. For example:



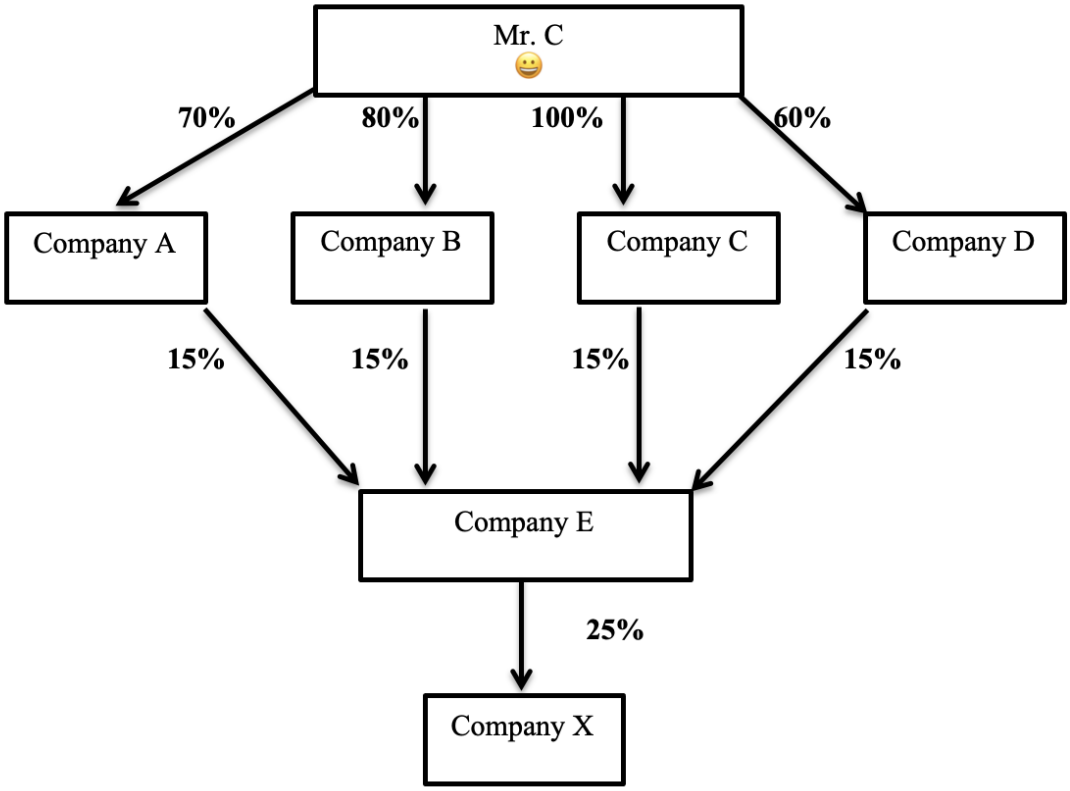
In the above example, "Mr. C" has a majority stake (60%) in Company C, which has a majority stake (70%) in Company B, which owns 80% of Company A, which holds 25% of Company X. Because there is an unbroken chain of majority stakes in the corporate shareholder (Company A) that owns 25% of Company X, Mr. C would be considered a BO of Company X.

The following example shows a different result:



In the above example, "Mr. C" has a majority stake (60%) in Company C, but Company C does not have a majority stake (only 40%) in Company B, the 20% owner of Company A, which holds 25% of Company X. Because there is not an unbroken chain of majority stakes in the Company A, which that owns 25% of Company X, Mr. C would be not considered a BO of Company X based on ownership. Note, however, that Mr. C could still be considered a BO of Company X if he satisfied one of the "control" tests described below.

A person may hold beneficial ownership through multiple entities within an ownership layer. The following example illustrates this point:



In the above example, "Mr. C" has a majority stake in each of 4 companies, each of which holds 15% of Company E, which owns 25% of Company X. Mr. C would thus be considered a BO of Company X: he controls (via his majority stake) 4 companies, which collectively own 60% of Company E, the corporate shareholder of 25% of Company X.

The Multiplication Test

In contrast to the majority stake test, the multiplication technique determines ownership by simply multiplying the ownership percentages.

In the first example in the "majority stake" section above, multiplying the ownership percentages results in "Mr. C" having a 10.5% indirect ownership stake in company X (25% X 60% X 70% = 10.5%). Because the ownership test for BO status is 25%, Mr. C would not be considered a BO of Company X under the "multiplication" test.

However, it is quite clear that Mr. C can, in substance, control how Company A's 25% of Company X's shares are voted: by holding a majority of the shares in Company B, Mr. C can control the composition of Company B's board of directors, which normally would determine how 60% of Company A's shares are voted. Company B can, therefore, control the composition of the board of directors of Company A, which would determine how Company A's shares (here, 25%) of Company X are voted. Stated differently, Mr. C can do, relative to Company X, what a 25% shareholder can do.

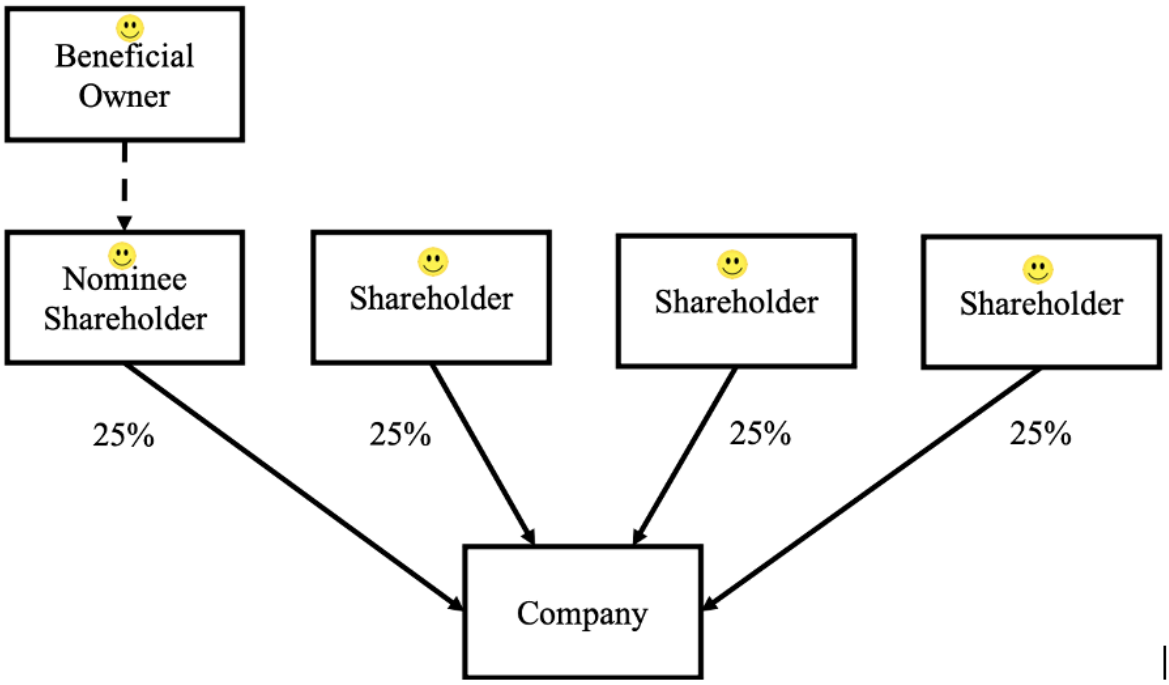
The multiplication test is unsatisfactory by itself for determining BO, as it focuses only on the size of the shareholdings but disregards real ability to effectuate voting rights. However, it can

be useful for those situations where the majority stake test is not applicable due to the lack of an unbroken ownership chain.

Nominee Shareholders

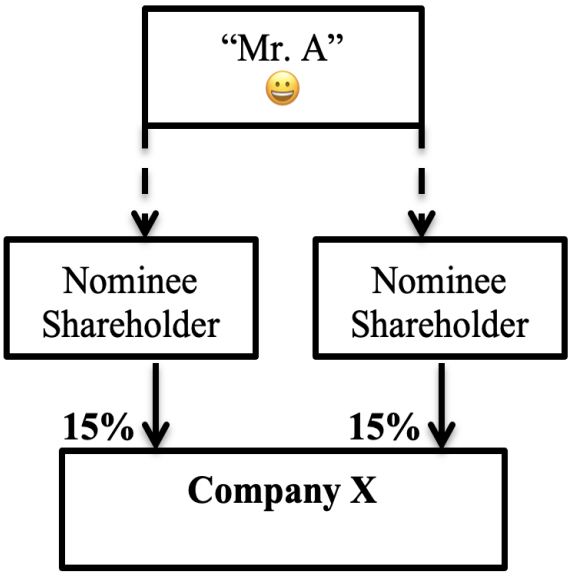
A natural person shareholder might hold shares as "nominee" for another natural person. The legal shareholder may hold the shares in trust for that underlying natural person, or the underlying natural person may simply wish to keep his or her ownership hidden (even if there is no actual trust agreement, or any other formal contract or agreement). The person holding the shares in this situation is the legal owner and the person for whom they hold the shares is the BO. If that BO holds at least 25% of shares of the company in this manner (either entirely through such an arrangement, or in any combination of legal and beneficial ownership), that person is considered to be a BO of the company.

In the following example, the company has 4 natural person shareholders, 3 of whom hold the shares for themselves, while the fourth holds the shares for someone else. Because all 4 shareholders are legal owners of 25% of the company, they are both legal and beneficial owners. There is also an individual for whom the nominee shareholder holds shares.



In the above example, there are 5 BOs: the 4 "legal" 25% shareholders, and the BO of the shares held by the "nominee" shareholder.

A person might be the BO of a company through more than one nominee shareholder, even if all of the nominee shareholders would not be considered BOs based on their legal ownership. The following simple example illustrates this point. In this example, there are two 15% shareholders who are nominees for "Mr. A," who formally owns no shares in the company at all:



In this example, "Mr. A" must be considered a BO of Company X, because his total beneficial ownership amounts to 30%, despite being held by two different nominee shareholders.

The Control Component

In determining beneficial ownership of a legal person or legal arrangement customer, the FI should look beyond formal (direct or indirect) ownership and should examine ultimate effective control. "Control" of a legal entity or arrangement can be exercised in a number of different ways, including extortion, coercion, or merely through secret agreements between an entity's managers or directors and the actual controlling person.

Examples of ultimate effective control over a legal entity include:

- the power (whether formalized or not) to appoint a majority of the members of the board of directors of the entity, or in the case of a company, the board of directors of a parent company of that company;

- the person's representatives or nominees constitute a majority of the members of the board of directors of the entity, or in the case of a company, the board of directors of a parent company of that company;

- the person has such controlling power pursuant to an agreement with the company, or a provision in the constitutive documents of the company, or in a parent company of that company, such as the charter, articles of association, or any similar document;

- a majority of the members of the board of directors of the company, or of a parent company of that company, or the senior managing official of that company or parent company, are accustomed or under an obligation, whether written or unwritten,

formal or informal, to act in accordance with the instructions, directions, or wishes of a given natural person in conducting the affairs of the company; or

- a person makes recommendations to the shareholders or members of the company, or of a parent company of that company, on matters requiring shareholder or member approval, and these recommendations are always or almost always followed by shareholders or members holding at least 25% of the voting rights in that company or parent company, when they are deciding how to vote.

Some persons can exert a considerable degree of influence on a legal entity or arrangement through the provision of professional services. Because of the nature of these relationships, these persons should not be considered to be BOs based on that relationship alone. A BO therefore would not include a natural person in accordance with whose directions, instructions or wishes the directors, partners, or senior managing officials, or persons in equivalent positions of any entity are accustomed to act, or whose recommendations are customarily followed, solely based on advice given by that person in his or her professional capacity. Such persons could include, for example:

- a lawyer;
- an accountant or auditor;
- a management consultant;
- an investment manager;
- a tax adviser; or
- a financial advisor.

Because FIs do not have the same kinds of resources or investigative powers as supervisory or law enforcement authorities, they are not expected to conduct detailed investigations to determine the existence of undisclosed or "secret" beneficial owners. However, they should make inquiries of potential customers at the time of account opening or prior to executing an occasional transaction. For this purpose, it is a good business practice to require each customer, and in particular each legal entity or legal arrangement customer, to verify its BO(s) for each account or prior to carrying out an occasional transaction.

"Acting in Concert"

Both the ownership and control components of the BO concept must consider the possibility that ownership or control can be achieved through persons acting together.[12] FASU Guidance recognizes this by noting that "control" includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, where or not having legal or equitable force and whether or not based on legal or equitable rights. In international practice this is often referred to as "acting in concert."

[12] FATF Recommendation No. 10, par. 5(b) (referring to persons "acting alone or together" who exercise control of a legal person or arrangement); FATF, *Transparency and Beneficial Ownership* (October 2014), p. 15 (referring to "shareholders who exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity).

"Acting in concert" generally can be defined as "a conscious course of parallel action taken by two or more persons, in accordance with any agreement, commitment or understanding, whether formal or informal, verbal or written, to act jointly or in combination with each other with a view toward achievement of a common objective." Persons are often presumed in certain circumstances to be acting in concert with each other unless it is shown otherwise. The following are examples of relationships that should be presumed to involve concerted action:

- A legal person should be considered to be acting in concert with a controlling person of that legal person.

- A person should be presumed to be acting in concert with his or her close family members (i.e., spouse, parents, grandparents, children, grandchildren and siblings).

- Legal persons in the same group (i.e., parent, subsidiary and sister companies) should be presumed to be acting in concert with each other.

- Legal persons that are controlled by the same person (legal or natural) should be presumed to be acting in concert with each other.

- Persons should be presumed to be acting in concert with each other relative to a legal person ("Entity A") where -

  – they are both members of the board of directors, senior management officials, or controlling persons of the same legal person other than "Entity A;" or

  – one person provides credit to the other person or is instrumental in obtaining financing for the other person to purchase shares of Entity A (other than a situation where one such person is a financial institution that provided credit to the other person to purchase the shares in the ordinary course of business and holds a security interest in the shares so purchased).

- The trustee of a trust should be presumed to be acting in concert with the trust and with the beneficiaries of the trust.

- Beneficiaries of a trust should be presumed to be acting in concert with the trust and with each other.

- General partners in a partnership should be presumed to be acting in concert with each other and with the partnership.

At the same time, not every situation of persons acting in a similar manner necessarily indicates that those persons are acting in concert. Examples include:

- discussions with each other about possible matters to be raised with their company's board or management;

- making representations to a company's board or management about company policies, practices or particular actions that the company might be considering;

- exercising shareholders' legal rights in the same manner with regard to items such as:

  - adding items to the agenda of a general meeting;

  - recommending draft resolutions for items included or to be included on the agenda of a general meeting; or

  - proposing to call a special meeting, apart from the annual general meeting;

- other than in relation to appointment of members of the board, agreeing to vote in the same way on a particular resolution put to the general shareholders' meeting, such as, for example, votes on proposals regarding:

  - directors' remuneration;

  - an acquisition or disposal of assets;

  - a reduction of capital and/or share buy-back;

  - a capital increase;

  - a dividend distribution;

  - the appointment, removal or remuneration of auditors;

  - the appointment of a special investigator;

  - approval of the company's financial statements;

  - the company's policy in relation to major social or political questions; or

  - approval of related party transactions.

In addition**,** persons need not be presumed to be acting in concert relative to a given entity solely because:

- they both serve as members of the board of directors or senior management officials of that entity;

- one of them is a proxy holder for one or more of the others regarding the voting of shares at an annual or special shareholders' meeting in accordance with applicable securities legislation; or

- they independently exercise voting rights attached to shares or ownership interests in that entity in the same manner.

Where No Beneficial Owner Can Be Identified Based on Ownership or Control

There may be some cases where no natural person who ultimately owns or exerts control over a legal entity or arrangement can be identified based on the above criteria. In such cases, FIs may consider one or more senior managing officials (such as the Chief Executive Officer) to be the BO(s). This, however, should be done after the FI is satisfied that it has exhausted all other means of identification, and that there are no grounds for suspicion. The FI should keep records of the actions it has taken to identify the beneficial ownership.

Ownership/Control Structure: Legal Entities

For companies with multiple layers in their ownership structures, FIs should take reasonable measures to verify the identity of the BO, and understand the ownership and control structure of that customer. This means, among other things, that any intermediate layers of the company's ownership structure should be fully identified. The manner in which this information is collected should be determined by the FI and incorporated into its policies and procedures. An effective means of doing this is to obtain a declaration from a senior official (such as the chief executive officer or corporate secretary) of the entity incorporating or attaching an ownership chart or organogram clearly showing the ultimate parent company (if any), each intermediate company, and the respective ownership of each company, including the ownership interests of the beneficial owner(s).

The amount and degree of detail of the information to be included should be determined on a risk sensitive basis, but at a minimum should include company name and place of incorporation, and where applicable, the rationale behind the particular structure employed. The objective should always be to follow the chain of ownership and actual effective control "all the way to the top," i.e., to the individuals who are the ultimate BOs of the direct customer, and to verify the identity of those individuals.

It is usually not necessary for FIs to routinely verify the details of the intermediate companies in the ownership structure of a company. Usually the names, locations and type of businesses of the companies, and their respective ownership will be sufficient. However, complex ownership structures (e.g., structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk. In these cases, further steps may be necessary to ensure that the FI is satisfied on reasonable grounds as to the identity of any BOs.

The need to verify the intermediate corporate layers of the ownership structure of a company will therefore necessarily depend upon the FI's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the FI to consider if it has taken adequate measures to identify the BOs.