FINANCIAL INTELLIGENCE CENTRE

SUMMARY OF FIA COMPLIANCE ASSESSMENT & NPO SUPERVISION METHODOLOGY

First issued: May 2016

First update: February 2019

Second update: March 2021

Third update: January 2023

Fourth update: June 2023

Fifth update: December 2024

TABLE OF CONTENTS

1. INTRODUCTION

The primary mandate of the Financial Intelligence Centre (FIC) is to contribute towards safeguarding the integrity of the Namibian financial system. The FIC's efforts geared towards fulfilling this mandate are mainly guided by various provisions such as section 9(1)(h) of the Financial Intelligence Act 2012 (Act No. 13 of 2012) as amended (FIA), the Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No 4 of 2014) (PACOTPAA) and to a certain extent, the Prevention of Organised Crime Act, 2004 (Act No. 29 of 2004) (POCA).

The various divisions within the FIC are structured to ensure advancement of relevant objects as per the said laws. The Compliance Monitoring and Supervision Division (CMSD) in particular has a duty to supervise, monitor and assist in enhancing effective functioning of controls within Accountable and Reporting Institutions (AIs/RIs) to mitigate Money Laundering, Terrorism and Proliferation Financing (ML/TF/PF) risks. An integral part of this function lies in the FIC supervised populace (AIs and RIs) complying with the FIA, any regulations, directives, guidance, determinations, notices or circulars issued in terms of such law.

Central to FIC's CMSD activities lies the need to gain reasonable assurance that AIs and RIs are effectively mitigating ML/TF/PF risks and thus complying with the FIA, and where need be, with the PACOTPAA and POCA. Such assurance functions are embodied in compliance assessments (similar to audits or inspections) and such similar activities which are explained herein. The said assessment activities enable the FIC to, amongst others:

a. appreciate the level of risk mitigation at entity and sectoral level;
b. identify ML/TF/PF risks (threats and vulnerabilities) and thus cause the necessary intervention (guidance, training, enforcement, or other mitigation efforts etc.); and

c. impact the reporting behaviour of the FIA supervised populace with focus on ML/TF/PF risk mitigation and enhancing the quality and timeliness of reports reaching the FIC.

In furtherance of the above, the FIC primarily assesses the adequacy and effectiveness of an NPO, AI, RI's Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation (AML/CFT/CPF) risk management system (internal controls). This document outlines the FIC's methodology and approach in such regard.

The overall result of effective ML/TF/PF risk mitigation is enhanced integrity and stability of the financial system. It is this result which lies at the center of all CMSD activities of the FIC.

1.1 JANUARY 2023 UPDATE

The January 2023 update aimed to align supervision activities with findings in the country's Mutual Evaluation.

1.2 JUNE 2023 UPDATE

The June 2023 update of this document, while building on the January update, simply clarified ratings/risk level of environments associated with implementation of Targeted Financial Sanctions (TFS). The January 2023 update spoke to sanctions screening without duly extending to the core TFS measures as required in law. See additional explanation around measures in the table on effectiveness ratings on page 18 and the amended part J(iii) on page 33.

1.3 AUGUST 2023 UPDATE

Within this context, 'NPO supervision' speaks to all FIC activities aimed at monitoring and outreach activities of NPOs. While the FIC has registered and supervised NPOs since

2019/20, the supervisory and outreach activities were not limited to one document. In the main, directives were issued and other publications were effected on the FIC website and in the mainstream media explaining risk management requirements. The FIC's supervision activities have largely been to help NPOs appreciate such risk management requirements as documented in various publications. The August 2023 update explains the NPO monitoring and outreach regime as per the FIA.

2. PURPOSE

The FIC has a structured and consistent methodology used to gauge the level of effective functioning of AML/CFT/CPF controls within AIs and RIs and thus FIA compliance. An understanding of such levels of control effectiveness enables the FIC, as a supervisory body, to determine the level of assurance to place on controls within assessed AIs and RIs. This document presents a high-level outline of such FIC assessment methodology. The presentation of this outline can add value by:

a. enhancing AIs and RIs' understanding of the FIA compliance assessment methodology; and thus
b. enhance the ease with which the FIC and assessed AIs/RIs engage on FIA compliance assessments. This should essentially help institutions plan and prepare for compliance assessments and understand if the FIC is consistent with its own methodology, amongst others. It is for this reason that this document is published and openly shared.

3. SCOPE

The FIC's CMSD activities include a wide range of functions such as availing guidance, conducting assurance activities, assessing sectoral and national ML/TF/PF risks to inform supervision, amongst others. As mentioned above, this document serves to focus on the FIC's methodology employed for conducting assurance activities. The methodology explained herein is applicable to all activities conducted by the FIC in assurance related activities. These activities include, but are not limited to the following:

a. conducting FIA Off-Site and On-Site compliance assessment activities;

b. ratings or considerations (conclusions/findings) used to gauge the level of sectoral and institutional risk mitigation[1] during Onsite and Offsite FIA Compliance Assessments;
c. reviewing periodic progress reports submitted by AIs and RIs;
d. any other relevant FIA Compliance Monitoring and Supervision activities; and
e. considerations for sanctions to enforce compliance as per the FIA.

4. METHODOLOGY

4.1 Coverage: Assurance Activities

Since the commencement of the FIC's Compliance Monitoring and Supervision activities in 2012, there has always been over 1,000 (one thousand) AIs, RIs and NPOs under its supervision as per the FIA. The number of supervised entities that register with the FIC keeps growing year-on-year. All such institutions should be subjected to the necessary supervisory activities as per FIA requirements. Given this extensive volume of supervised entities, the Risk Based Approach (RBA) is essential in ensuring due and effective coverage. The methodology used to select institutions to be subjected to assurance activities is informed by various factors including:

a. FIC's periodic AML/CFT/CPF supervision plans and strategies informed by risks: the level of ML/TF/PF risk exposure in such AIs/Ris/NPOs and/or the sector as per various considerations including:
    - Sectoral Risk or Vulnerability assessments;
    - periodic supervisory risk reviews; and
    - reported cases of vulnerabilities or actual risk materialization etc.;
b. supervisory sectoral coverage levels;
c. progress made in implementation of remedial measures (e.g. from previous assessment related activities, periodic progress reports);
d. reporting behavior[2] of the AI/RI/NPO; and
e. any other factors/information deemed relevant to consider.

[1] Control effectiveness
[2] STR, SAR, CTR, EFT, IFT reports etc. that are supposed to be reported to the FIC.

The RBA allows the FIC to direct the utilization of its limited resources prudently given the vast supervised populace countrywide. The level of ML/TF/PF risk exposure in an institution, based on the nature of its clients, product/service distribution channels (incl. geographical reach), nature of products and services, usually informs the nature, extent and routine of the supervision and monitoring activities to be conducted. The FIC, on an annual basis drafts a supervision plan which includes identification of AIs/RIs to be assessed yearly. As mentioned above, various factors including national, sectoral and entity level risk exposure as well as sectoral supervisory coverage[3] informs such supervision plans. To the extent possible, inputs from relevant stakeholders including prudential regulatory/supervisory bodies are considered in such supervision plans. Where possible, joint assessment activities with prudential or other supervisory bodies are considered.

Ad-hoc FIA compliance assessment activities are often carried out when information comes to the attention of the FIC necessitating immediate or ad-hoc assessment/assurance activities. In such assessments, there is usually deviation from this framework, depending on review/investigative/assessment objectives.

4.2 Nature of FIA Compliance Assessment Activities

4.2.1 Major areas of FIA Compliance Assessments

The **scope** of FIA compliance assessment tests/reviews is generally limited to provisions within the FIA and the extent to which such requires consideration of other relevant laws such as the PACOTPAA, POCA, Companies Act etc., in attainment of assurance related to ML/TF/PF risk mitigation. The major FIA provisions against which AML/CFT/CPF controls in AIs and RIs (and NPOs, to the extent required as per the new FIA section 35) are assessed/measured include, but are not limited to the following:

a. ML/TF/PF risk assessments done on products and services offered by the AI/RI, in consideration of its clients/customers *(Section 20A, 35 and NPO Regulations)*;

[3] especially with low-risk entities

b. Customer Due Diligence (CDD) / Know Your Customer (KYC) (Sections 21 & 22);
c. The identification and risk management procedures of risk clients (Section 23);
d. Record keeping (Section 26);
e. Account/transaction/client monitoring (Section 24). This highly impacts the ability to detect, prevent and/or report as per FIA Section 33;
f. Compliance with sanctions screening obligations as per FIA Sections 23, 24 and the PACOTPAA regarding compliance with United Nations Security Council (UNSC) Resolutions;
g. The identification, due diligence and on-boarding of Correspondent Banking Relationships (Section 25);
h. Reporting of suspicious transactions/activities (Sections 33);
i. Filing mandatory reports such as Cash Threshold Reports (CTRs), Electronic Funds Transfer (EFT) reports etc. – primarily as per FIA, read with Circular 03 of 2015 (Section 32);
j. AML/CFT/CPF awareness raising and training of staff (Section 20A (6) (b); and
k. Independent review/audit of AML/CFT/CPF controls (Section 20A (6) (c)).

Annexure A (read with sections 4.2.5 and 4.2.6) of this document avails demonstrations of how the FIC arrives at its observations or findings in terms of the above-mentioned sections of the FIA.

4.2.2 Monitoring Activities

In addition to the assurance gaining activities explained above, the FIC equally conducts compliance behavioral monitoring activities. Such activities may include:

a. continuously assessing ML/TF/PF risks at AI/RI/NPO, sectoral and national levels;
b. reviewing reporting behavior at AI/RI/NPO, sectoral and national levels;
c. reviewing periodic progress reports from AIs/RIs on control related remedial actions undertaken; and
d. consideration of information/data from external sources that have a bearing on risk exposure in AIs/Ris/NPOs.

4.2.3 Assurance Functions in Supervisory Activities

Supervision activities can entail various mechanisms that any supervisory authority deem necessary to attain supervisory objectives. In this regard, this document focuses on FIA compliance assessment activities which are exercised to gain supervisory assurance on the effectiveness of AML/CFT/CPF controls within AIs and RIs. The FIC employs measures to assess how AIs and RIs comply with the legal requirements set out in the FIA, POCA, PACOTPAA and their Regulations. Such assessment activities are either executed Onsite or Offsite. Onsite and Offsite assessment activities can be explained as follows:

a. **Offsite**[4] – mostly conducted by FIC staff members reviewing an AI/RI's/NPO relevant data/information without necessarily being on the business premises of the assessed AI/RI/NPO; and
b. **Onsite** – this refers to FIC staff members being physically 'on-the-site' or business premises of assessed AIs/Ris/NPO.

It should be further noted that many a times, an assessment activity could entail both Offsite and Onsite assessment activities. The FIC staff members would have the prerogative to decide on the most suitable approach to enable testing control adequacy or effectiveness and the extent of such (substantive tests), usually informed by risk considerations. When need be, these assessments might be conducted jointly with other supervisory bodies, such as the Bank of Namibia, Law Society of Namibia and/or Namibia Financial Institutions Supervisory Authority (NAMFISA), in an effort to streamline supervisory and combined assurance efforts. In advancing the integrity of the financial system, outcomes from FIA compliance assessment activities may be shared with relevant authorities such as prudential supervisory bodies as per section 9 of the FIA.

The next subsection presents a brief outline of such Offsite and Onsite Assessment activities.

[4] Note that the reviewing of progress reports on remedial measures post a compliance assessment activity is included in the scope/definition of offsite activities.

4.2.4 Offsite FIA Compliance Assessments

All assessment activities commence with the FIC issuing a formal or informal notification to the AI/RI/NPO to be subjected to such assessment.

With Offsite assessment activities, the FIC obtains or requests certain information from the AI/RI/NPO or any other entity/authority and reviews the same from the FIC office (desk reviews). These desk reviews are usually not conducted on the premises of the assessed AI/RI/NPO. Under normal circumstances, Offsite compliance assessment activities entail desk reviews of relevant information to gain assurance on the existence, design and adequacy of AML/CFT/CPF controls. With such assurance levels, the aim is to help the FIC consider other suitable supervisory or AI/RI/NPO interventions to enhance controls, if need be. As a norm, most (if not all) Onsite assessment activities commence with Offsite reviews that inform execution of Onsite activities.

The level of effective functioning of controls may not always be readily ascertained with Offsite assessment activities. Such control effectiveness testing is usually done with Onsite assessment activities. It should however be noted that in certain circumstances, relevant observations from Offsite assessment activities could give indications of control effectiveness levels.

In a structured Offsite assessment activity, the FIC requests data/information using data collecting tools such as questionnaires, supervision templates etc. In unstructured Offsite approaches, the FIC requests data/information via email, formal letters etc. Importantly, the FIC, depending on the assessment objectives and nature of activities being assessed, could include certain Onsite activities in an Offsite engagement and vice-versa. Offsite assessments are often less demanding on the resources of assessed AIs and RIs. These type of assessment activities are mostly conducted on medium-to-low risk institutions and sectors. The FIC also uses this type of assessment for targeted assurance activities when the need arises.

When Offsite assessment activities are carried out, certain outcomes/observations come to the fore. Based on such assessment outcomes, the FIC may consider:

a. requesting further information needed for the assessment;
b. taking other actions such as:
    i. providing guidance on necessary remedial measures;
    ii. scheduling Onsite or other type of compliance assessments/reviews;
    iii. availing training on FIA compliance; and
    iv. any other interventions the FIC may deem appropriate, in line with the FIA and other relevant laws, necessary to enhance compliance.

Unless findings suggest otherwise, the Offsite compliance assessment activity ends with the issuing of a formal compliance assessment report. If need be, and depending on the nature of the assessment, such report is finalized and presented after considering inputs from the assessed entity.

4.2.5 Onsite FIA Compliance Assessment Activities

Under normal circumstances, the Onsite FIA compliance assessment activity is the highest assurance providing activity conducted by the FIC. It entails a pre-assessment planning phase (usually in the form of an Offsite review), followed by execution of the actual Onsite assessment and normally ends with the presentation of a compliance assessment report. The following section avails a description of the approach adopted in Onsite assessment activities:

Planning

a. The compliance supervision team (herein referred to as team) will notify the AI or RI via email, or a Notification letter in advance of the FIC's intention to conduct an assessment activity. Usually, such notification should reach the AI or RI at least a week (5 working days) before the actual assessment activity commences, except where circumstances dictate that a shorter notice (or no notice at all) be availed especially when such Onsite assessment is a targeted/investigative or ad-hoc assessment activity;

b. The notification letter is usually accompanied by a Planning Memo detailing the scope of the assessment, the timelines, objectives and deliverables. Depending on the nature of the assessment, the FIC would, in such planning memo indicate or request the data/information needed for assessment purposes (for sampling purposes, preliminary testing and reviews etc.). Other information usually required at the planning stage includes transactions for a certain period under review, FIA compliance programs and risk assessment documents;

c. During this phase, the team can also arrange for meetings with the AI or RI to discuss the assessment and provide clarifications regarding the scope and/or requested information;

d. Depending on the nature of the assessment, selected information is usually sent to the AI or RI to prepare records, information and files for the actual assessment.

e. Further, depending **on the level of sectoral and entity risk exposure** for the particular AI or RI to be assessed, the sampling of transactions will take into account, but not limited to factors such as:

- Identified high risk areas, including clients, products, geographical areas, and transaction modes;
- Level of cash transactions (or such vulnerable services) in the business modules of the AI or RI;
- The volumes of **transactions** in different services and products of the AI or RI or by a specific client;
- The level of engagement in inherently high-risk services such as international cross border remittances in line with identified risks as per Revised Directive 1 of 2016 or any such other relevant guiding document;
- AI/RI information related to behavioural or transactional monitoring and reporting;
- Different transaction behaviors of clients including trends and typologies.

Field work and Reporting

a. The field work phase of the assessment is normally preceded by an opening meeting, usually with the relevant management and the Anti-Money Laundering Compliance Officer (or department) of the institution. This meeting is set to discuss the objectives of the assessment and enhance the FIC's understanding of the operations in the business units to be assessed. This also enables the assessed entity to enhance its understanding of the planned assessment activity. Management of the section(s) under review will normally highlight the high risk areas and indicate how they are mitigating same;
b. The field work entails mainly testing/reviewing selected transactions or business relationships to understand how relevant AML/CFT/CPF controls have or are mitigating relevant risks in terms of the FIA;
c. **The AIs/RIs are entrusted with compliance obligations. Thus, the FIC's approach is premised on selecting transactions or business relationships and querying the relevant processes or business units etc., to understand risk mitigation (FIA compliance). The assessed entity has the responsibility to demonstrate how it is complying with the law, as per FIC selected or queried transactions/clients.**
   - For selected transactions, the AI or RI need to, amongst others, demonstrate the following to the FIC:
     - ✓ Does the transaction meet the selected clients' financial profile?
     - ✓ What is the risk rating or consideration? Could the transaction be considered a high risk transaction?
     - ✓ Did the AI or RI obtain and understand the source of funds for the transaction? Is such in line with client profile?
     - ✓ Did the AI or RI report the transaction to the FIC, if not, is there rationale for not reporting same?
     - ✓ Was the transaction above the threshold (e.g. CTRs) and was it reported, if not, is there rationale for not reporting? If reported, proof that same was reported timely;
     - ✓ Was this a cross-border transaction, if yes, was due diligence conducted in terms of required provisions, Revised Directive 01 of 2016 etc.?
   - For selected business relationships, the AI or RI needs to demonstrate the following to the FIC:
     - ✓ What is the level of risk presented by the client as per the AI or RI? Is the risk rating supported by relevant factors?
     - ✓ Did the AI or RI conduct sufficient due diligence, based on the level of client risk exposure?
     - ✓ Does the AI or RI have an updated client profile commensurate with the transactions concluded?
     - ✓ Did the AI screen the client against relevant United Nations Security Council Sanctions Lists upon take-on or account opening, and whenever such Lists are updated? Was such screening done within prescribed timelines?
d. AIs and RIs remain charged with a duty to demonstrate effective risk mitigation as per the FIA, to the FIC and the FIC draws conclusions based on such demonstrations;
e. Material exceptions will normally be highlighted to management during the reviews/assessments;
f. After testing, the assessment team will call for an exit/closing meeting with management to discuss the exceptions noted (draft assessment report, if available); This platform enables management to give inputs and if need be avail further information. Depending on the nature of the assessment and its objectives, the FIC has discretion on how to treat such inputs;
g. Assessment findings are discussed in the closing/exit meeting. The draft assessment report or summary of findings is presented for such discussions. This exit meeting occurs **within 5 working days** after finalizing the assessment. Management must avail inputs, if any, **within 5 working days** of discussing or receiving such draft report;
h. The final report is presented **within 10 working days** from the day management inputs are received, unless otherwise communicated. Assessment formally ends when final report is presented. Such report, amongst others, directs the AI or RI to periodically report progress, for post assessment monitoring, on the implementation of remedial measures.

Remedial Measures and Progress Tracking *(post assessment monitoring)*

i. During this phase, the assessed AI or RI avails periodic reports, as stated in assessment report, on progress made in implementing remedial measures (such reports could be availed quarterly or as indicated by the FIC);
ii. The FIC reviews such remedial measures as presented, in view of report findings and gauges how such could mitigate ML/TF/PF risks. The FIC may seek an audience with the AI/RI if need be or decide to conduct any other suitable measures, including additional assessments, to gain assurance;
iii. After reviewing progress reports, the FIC indicates its position and any further recommendations if need be, **within 10 working days** of receiving such progress report;
iv. As the AI/RI reports periodically on remedial measures employed, the FIC may advise that such AI/RI cease with the periodic reporting when satisfied that such further periodic reporting is no longer necessary;
v. As most reviews on periodical reporting is conducted Offsite, the FIC is usually only able to test practical control effectiveness in future Onsite assessment activities or such other tailored reviews; and
vi. To the extent that unmitigated or poorly mitigated risks are known, the supervision team may refer the assessed AI/RI for enforcement considerations in terms of its internal policies and procedures, regardless of whether such was done with the final compliance assessment report. Reporting on assessment findings/observations does not take away from the FIC's continued responsibility to gain assurance that timely and effective risk mitigation interventions are considered at all times. Thus, the FIC may exercise any intervention it deems necessary during such period to gain assurance around effective risk mitigation.

4.2.6 Compliance Ratings Assigned

The January 2023 revision of this methodology, which was partly informed by supervised sectors calling for a mechanism to rate the levels of risk mitigation (in each assessment) in order to best reflect progress (if any), that assessed entities may be making. The assessment methodology did not previously rate findings on a given scale to show the level of control effectiveness. This is also essential in helping to demonstrate the impact of the FIC's supervisory activities as per FATF Immediate Outcome 3 of the Mutual Evaluation Methodology.

ML/TF/PF risks are critically relevant to evaluating compliance with the FIA obligations. The FIC will consider the nature, severity and impact of the shortcomings identified, along with entity and sector level ML/TF/PF risks, in arriving at its conclusions or observations.

The FIC, in its monitoring and supervision activities aims to counter against the materialization of ML, TF and PF risks within the ambit of an AML/CFT/CPF framework. Whilst materiality of compliance failures are considered, the essential guiding principle of findings raised is the nature, severity and impact of exposure to ML/TF/PF vulnerabilities (control weaknesses) and threats (potential of activities to undermine such vulnerabilities). For example, high risk[5] environments or services have lower tolerance levels for control failures. The FIC's supervision function does not have authority to condone non-compliance with the law. Generally, courts or such relevant administrative enforcement function as per the FIA has authority to condone or duly deal with poor risk mitigation and thus non-compliance observed by the supervision function. This is the guiding principle within a Financial Intelligence Unit's supervisory framework.

With the above in mind, tests of controls in high-risk environments or areas such as sanctions screening, transactions conducted by PEPs, cross border remittances etc., would be adequate to reveal compliance behaviour with minimal or no substantial tests

[5] AIs/RIs are expected to duly and accurately assess risks with regard to threats and vulnerabilities, guidance from the FIC, and any other internal or external source. The FIC, if reasons exist, may disregard the risk ratings/classifications or findings of an AI/RI for supervision purposes.

required. This is because any failure in that space unduly exposes the assessed entity's services and thus the national financial system to ML/TF/PF risks. With medium to lower risks, given the need to have slightly less extensive controls in such areas, substantive tests may be considered to determine the extent to which failures may have occurred or the AI/RI has been exposed. The nature and extent of such substantive tests would be determined by the assessment team in order to arrive at viable and risk-based conclusions on risk management effectiveness within an AI/RI/NPO.

In arriving at conclusions, the FIC considers and weighs the shortcomings of an AI's controls in a given area and how such impacts on other compliance obligations. For example, the absence of a risk assessment will hinder the effective conducting of CDD, monitoring and thus resulting in the non-detection and failure to report unusual and suspicious transactions. Most often, the same underlying deficiency will have a cascading effect on the assessment of several different obligations.

As part of the FIC's assessment, the supervision function considers the exposure of not meeting a requirement. In so doing, assess the nature, relative exposure emanating from same, extent of the non-compliance (when need be, conduct substantive tests), and any mitigating or aggravating factors. **As the FIA compliance obligations fall on AIs and RIs, it is the responsibility of the AI or RI to demonstrate that its AML/CFT/CPF system is effective in risk mitigation and thus compliant with the FIA and its accompanying regulations, to the satisfaction of the FIC as the supervisory body.**

With regards to the ratings introduced with the January 2023 update of this methodology, assessments of the designs of controls as documented in policies and procedures would be regarded as assessments to determine the level of **Technical Compliance** with the FIA or AML/CFT/CPF framework. On the other hand, reviews on the practical functioning of such controls would speak to risk management **Effectiveness** of such controls. Given this, Offsite assessments would primarily be geared towards determining Technical Compliance levels. Onsite assessments, given their review of practical risk management efforts, would mostly be aimed at ascertaining the level of Effectiveness. Exceptions

however exists where Offsite assessments could yield outcomes around effectiveness (and vice versa for Onsites) when testing mechanisms are so designed. The sections below detail how assessment findings would be rated or categorized.

4.2.6.1 The ratings to be assigned to the findings/observations in terms *of Technical Compliance* with the FIA are as follows:

Compliance Rating	Description of rating	Extent of exposure
a) Compliant	There are *minor to no shortcomings* in the Policies, Procedures and other internal documents in line with the nature of business of the AI/RI/NPO.	The institution has covered most, if not all the technical compliance required by the legal framework, Regulations and Directives etc., in its compliance policies and procedures. The minor shortcomings, if any, should be insignificant and negligible, or of such a nature that it does not unduly expose AI/RI/NPO to significant ML/TF/PF vulnerabilities.
b) Largely Compliant (LC)	There are *moderate shortcomings* in the Policies, Procedures and other internal documents in line with the nature of business of the AI/RI/NPO that need to be addressed timely.	The institution has only covered some of the major compliance expectations required by the legal framework, its Regulations and Directives etc.
c) Partially Compliant (PC)	There are *worrying and significant shortcomings* in the Policies, Procedures and other internal documents in line with the nature of business of the AI/RI/NPO that need to be addressed timely to ensure risk mitigation.	The institution has not demonstrated adequate technical compliance required by the legal framework, its Regulations, Guidance and Directives etc.

d) Non-Compliant (NC)	There are *major and/or significant shortcomings* in the Policies, Procedures and other internal documents in line with the nature of business of the AI/RI/NPO that need to be addressed urgently.	The institution does not have any policies, programs, or any of the technical compliance requirements as per the legal framework, its Regulations, FIC Guidance and Directives etc.

The FIC, in determining the level of compliance for each obligation tested, does not only assess whether the AI/RI's/NPO FIA Compliance Program and controls conforms to the FIA obligations, but also assess whether such measures are effectively implemented and consistently applied, in terms of its RBA. Effectiveness reviews are thus core to gaining reasonable assurance around practical risk mitigation.

4.2.6.2 The ratings to be assigned to the findings/observations in terms of *Effectiveness* of the AML/CFT/CPF controls are as follows:

Compliance Rating	Description of rating	Extent of exposure
a) High Level of effectiveness	There are *minor, negligible shortcomings* in non-high-risk areas.	a) **High risk environments:** With the exception of high risk factors/areas such as sanctions screening[6], the institution has demonstrated an effective level of **95% or more** in tested records. High risk environments include controls around sanctions screening and Targeted Financial Sanctions (TFS)[7], PEP clients/transactions, cross border remittances (especially linked to high-risk jurisdictions), high value[8] transactions etc. There are limited tolerance levels, if any, for compliance failures in

[6] See Directive 01 of 2022 on sanctions screening effectiveness thresholds.
[7] Compliance with sanctions screening obligations, freezing without delay and prohibition as per FIA Sections 23, 24 and 25 of the PACOTPAA regarding compliance with United Nations Security Council (UNSC) Resolutions. See Directive 01 of 2023 and Guidance Note 07 of 2023.
[8] High value is based on impact, overall risk, nature of service, and client profile.

		high-risk areas (controls, clients, products/services or transactions). b) **Medium-Low Risk environments:** The control mechanisms tested/assessed are operating effectively as intended for the tests conducted in such environments, services or clients. **90% – 94% effectiveness level** from tested records could be reflective of a high level of effectiveness in Medium-Low risk environments. c) Shortcomings/failures or exceptions noted in high-risk areas could result in supervisory interventions including enforcement referrals, even if Medium to Low-risk controls are deemed effective.
b) Substantial Level of effectiveness	There are *moderate shortcomings* that need to be addressed timely.	a) The institution has demonstrated risk mitigation in **more than 59% of tested data but not more than 89%.** Note that this excludes high risk areas such as PEP clients/transactions, cross-border remittances etc. b) Overall, there may be significant compliance, but the tested control mechanisms (as a whole) may have moderate shortcomings (are below compliance tolerance levels). c) Depending on the severity, risk exposure and nature of non-compliance, this may require FIC intervention, including periodic progress reporting, and if need be, considerations for escalation to enforcement, or such relevant measures to enhance compliance.
c) Moderate Level of effectiveness	There are *major, worrying and significant shortcomings* that need to be addressed timely to ensure risk mitigation.	a) Significant and worrying shortcomings: The institution has demonstrated **more than 39% but not more than 59%** effective risk mitigation level as per tested records, outside of high-risk areas such as PEP clients, cross border remittances etc. b) The control mechanisms are not operating effectively as intended in the tested environments.

		c) This requires prompt FIC intervention, including enforcement considerations.
d) Low Level of effectiveness	There are *no controls or very negligible and insignificant controls in place.* There is an urgent need to timely implement effective controls.	a) The institution has demonstrated a **39% or less, effectiveness** risk mitigation level on the tested records, which are outside of high-risk areas. b) Inadequate or lack of controls: There are no control mechanisms, or such controls are insignificant, ineffective and severely expose the financial system to ML/TF/PF risks. c) Automatic referral for enforcement considerations unless convincing circumstances arise, such as the sector being completely new to the AML/CFT/CPF sphere (or recent amendments in laws, directives etc.) and AI/RI needs time to implement and grow or mature internal risk mitigation controls.

4.2.7 Addressing Poor Risk Mitigation Observations

The FIC's supervisory activities generally focus on working with accountable and reporting institutions to enhance their ML/TF/PF risk management systems and improve overall prevention and combatting mechanisms. The FIC aims to achieve this through capacity building, improving entities' understanding and capability in the area of ML/TF/PF risk management as per the FIA.

As mentioned in section 4.2.6 above, only courts (and such relevant administrative tribunals or platforms) have mandate to condone non-compliance with laws. The FIA avails platforms for sanctions and other interventions the FIC may explore as a regulatory body. The Compliance Monitoring and Supervision function is separate from the function entrusted with administrative enforcement of the FIA. When observations and findings around non-compliance are deemed necessary for enforcement referrals, the Compliance Monitoring and Supervision function does so as per internal referral policy framework.

In furtherance of minimizing poor risk mitigation, an assessment report may be escalated for enforcement consideration as envisaged in section 56 or such other relevant section of the FIA, due to observed poor compliance. Thereafter, the appropriate administrative sanctions may be considered by the relevant body within the FIC. The FIC, via its Enforcement function considers the merits of each case to determine the most appropriate intervention, including sanctions, to enhance risk mitigation, discourage poor compliance etc., as per enforcement framework.

4.2.8 Frequency of Institutional Supervisory Engagements

The FIC's periodic sectoral risk assessments, which are periodically updated, sets the entity risk level which guides the frequency, nature and extent of supervisory activities. Notwithstanding any information/factors which may come to the attention of the FIC necessitating deviation, the minimum frequency of supervisory engagements (assessments and/or monitoring activities) to gauge entity level risk mitigation shall be as follows:

Supervisory Entity Risk Profile	Assessment Frequency
High and Medium-High Risk entities	At least once every 1 – 2 years
Medium Risk entities	At least once every 3 – 4 years
Medium Low and Low Risk entities	At least once every 5 – 6 years

The above are minimum intervals and may only be deviated from with the approval of the Deputy Director, on reasonable grounds.

4.2.9 Finalization of Assessment and Monitoring Activities

4.2.9.1 Conclusion of compliance assessment

At the end of a compliance assessment report, observations are captured in a compliance assessment report. Before such final report is issued, a draft report is shared or summary

of findings are discussed with the relevant management[9] of the assessed institution in the closing/exit meeting. With some investigative reviews, this practice may not be adhered to, depending on the assessment nature and objectives. Assessment findings are discussed in the closing/exit meeting. The draft assessment report or summary of findings is presented for such discussions. This exit meeting occurs **within 5 working days** after finalizing the (onsite/offsite) assessment. Management must avail input, if any, **within 5 working days** of discussing or receiving such draft report. The FIC finalizes and issues the final report **within 10 working days[10]** from the date management inputs are received. The FIC will communicate delays, if any, in the finalization of assessment reports. The compliance assessment activity (Onsite or Offsite) thus formally comes to an end when the final FIA Compliance Assessment report is presented or handed over to the assessed institution. Such a report is transmitted via email or such other mechanism as may be deemed appropriate.

4.2.9.2 Commencement of *post-assessment* Monitoring Activities (progress reports)

At the end of the compliance assessment activity, if the FIC has observed findings which require implementation of remedial measures, the concerned institution is requested[11] to provide periodic progress reports indicating progress made in the implementation of such remedial measures, at each reporting interval.

4.3 Updating the Assessed Institution's Supervisory Risk Profile

A supervisory risk register, reflecting entity level supervisory risk, is to be maintained. An institution's ML/TF/PF risk profile is updated on such register at least once every 3 to 5 years, as per the outcomes of the sectoral risk assessment activity undertaken by the FIC at such intervals.

[9] Including the AML Compliance Officer appointed as per the FIA.
[10] +/- 4 days drafting and editing and +/- 4 days supervisory review and approval.
[11] The final compliance assessment report indicates the expected reporting periods, which are usually quarterly.

Notwithstanding any other factors observed outside of the conventional compliance assessment framework, the FIC will update each institution's risk profile (threats and vulnerability to ML, TF and PF) post the finalization of the assessment activity, or whenever any relevant information is noted. This is necessary to ensure the AML/CFT/CPF supervisory risk-based framework is periodically updated with the most recent considerations/factors relevant to institutional level risk management. Unless so required, the post-assessment entity level risk profile updating on the supervisory risk register shall therefore occur independent of the periodic sectoral risk assessment referred to above.

5 IMPACTS OF FINTECHS ON SUPERVISORY ACTIVITIES

The emergence of financial technologies (FinTechs) has not gone unnoticed within Financial Intelligence Units around the globe. In some cases, for effective compliance assessments to be conducted, some form of Regulatory Technology (RegTechs) is helpful. For example, VASP assessments/audits could require a VASP to demonstrate effective screening of wallets to fulfil assessment objectives (or the FIC could use RegTech tools to gain such assurance). To the extent possible, the principles adopted herein will be followed in the use of RegTechs, as done with the Thematic Reviews on effectiveness of sanctions screening solutions of financial institutions in 2021 and 2022.

It is expected that the use of RegTechs and SupTechs could redefine the conventional nature of supervision activities. For example, a typical Onsite assessment activity as described herein could be executed Offsite and still have the same impact.

Considerations are being made for AIs and RIs to avail information on certain platforms which will be used by the FIC for analysis, monitoring and other supervisory activities. Due awareness and communication in this regard will be considered at the appropriate time.

6 NPO MONITORING AND OUTREACH ACTIVITIES

6.1 Purpose of Monitoring

The FIC will undertake appropriate monitoring, review or assessment activities to understand the presence and/or extent of any of the following means (risks) of possibly abusing NPOs:

a. The **diversion of funds** is a significant method of abuse, with actors inside the NPO or external actors (such as foreign partners or third-party fundraisers) being responsible for the diversion to support terrorist entities at some point through the NPO's operational or financial processes;
b. NPOs or their directing officials knowingly or unknowingly **maintaining an affiliation with a terrorist entity** which may result in the NPO being abused for multiple purposes, including general logistical support to the terrorist entity;
c. Abuse to **support recruitment** efforts by terrorist entities;
d. The **abuse of programming** in which the flow of resources is legitimate, but NPO programs are abused at the point of delivery; and
e. **Abuse through false representation** in which terrorist entities start "sham" NPOs or falsely represent themselves as the agents of "good works" in order to deceive donors into providing support. Well-planned deceptions are difficult to penetrate with the resources available to non-governmental actors, making regulatory-based oversight and its capabilities a necessary element to detecting the most sophisticated threats to the sector's activities.

6.2 Major Governance and Risk Management Frameworks

The FIA Regulations as well as Guidance Notes 12 and 13 of 2023[12] provide the governance frameworks and related standards against which each individual NPOs' controls will be assessed, reviewed and measured by the FIC. Such assessment, review

[12] https://www.fic.na/index.php?page=2023-guidance-notes

or measurement will be aimed at gaining reasonable assurance that a NPO is not unduly vulnerable to risks as highlighted in section 6.1 above.

6.3 Registration with the FIC

NPO monitoring and supervision as per the FIA commences with registration. Amongst others, registration is a NPO's first opportunity to demonstrate how it plans to mitigate risks as per the FIA. The NPO's FIC registration regime is as contained in Directive 04 of 2023, available on the FIC website via Revised Directive No 4 of 2023 - NPO FIC Registration Regime.pdf. NPOs are required to demonstrate risk management measures as per the NPO Regulations.

Importantly, the supervision team conducts the first NPO entity level risk assessment (As per Annexure B of Revised Directive 04 of 2023) with the detailed information obtained during registration. NPOs that need not register with the FIC need to be issued a Clearance Certificate (as per Annexure C of Revised Directive 04 of 2023) as per FIA section 35.

6.4 Periodic Monitoring Activities

6.4.1 Risk Assessments

The FIC, as the supervisory authority of NPOs is required to conduct periodic risk assessments to understand TF risks at entity, sectoral, national and international level.

The FIC may therefore conduct sectoral or national risk assessments in the advancement of such objective. Outcomes thereof may, amongst others, be:

a. shared with the NPOs and relevant other authorities or stakeholders who can contribute to risk mitigation or combatting activities; and
b. used to inform the FIC's supervision, monitoring and outreach activities.

As part of risk assessments, the FIC may request or use relevant means to collect data and information from NPOs, other authorities and relevant stakeholders.

6.4.2 Annual NPO Returns

In addition to periodic risk assessments, the FIC will collect sectoral and entity level risk management data on an annual basis. Such data will be collected via the following two types of returns, at a minimum:

a. Annual NPO Returns – send to all or selected NPOs; and
b. Annual Banking Sector Returns – send to all or selected banks to enquire about the transacting behaviour of NPOs and banks' NPO risk management controls as per Directive 03 of 2023. See Directive 03 of 2023 - FIA Compliance Returns.pdf

The FIC will align annual returns to collect relevant data in view of prevailing risk considerations in the NPO sector. If need be, other means of sourcing data will be considered.

6.4.3 Targeted Interventions

The object of sourcing data via risk assessments, annual returns and other mechanisms is to obtain information which will inform the FIC's monitoring and outreach activities as stated herein above. Targeted interventions entail the following, amongst others:

Risk Level	Type of Outreach Activities	Frequency
Very High Risk NPOs – Especially those with cross border remittance activities	Monitoring of banking transactions every second month. Monitoring reports with findings, if any, should be produced. Annual review of banking sector returns and risk assessments. Review of Annual Financial Statements (AFS).	- Every second month cross border remittance monitoring activities. - Returns and AFS to be reviewed annually.

High Risk NPOs	Review of annual returns and banking sector risk assessments. If need be, escalate to off and onsite assessments.	Returns and risk assessments are reviewed periodically. *On and Offsite Assessments* will be undertaken as required.
Medium Risk NPOs	For medium risk NPOs, review returns and banking sector risk assessments every three years. If need be, escalation to offsite and possibly onsite assessment. For low risk NPOs, review of banking sector returns and risk assessments every five years.	
Low Risk NPOs		

Depending on the need and risk considerations, the FIC may amend the above or add to same as required to advance the objectives of the FIA.

6.5 Periodic Outreach Activities

Outreach Activities will be rolled out as follows, at a minimum:

Risk Level	Type of Outreach Activities	Frequency
Very High Risk NPOs	Media publications, one-on-one to smaller group training sessions (site visits). Tailored trainings based on outcomes of offsite reviews such as Annual NPO Returns and banking sector risk assessments.	Once a year
High Risk NPOs	Annual media publications; annually, review banking sector returns and risk assessments; sub-sectoral meetings.	Once every two years
Medium Risk NPOs	Annual media publications, sub-sectoral meetings. Tailored outreach activities depending on risk observations from monitoring activities.	
Low Risk NPOs	Annual media publications, sub-sectoral meetings.	Once every three years
Donors and Banks	Media publications on TF/NPO related risk management and sub-sectoral meetings.	

6.6 Enhancing Market Entry Measures

The FIC, in advancement of TF risk mitigation as per FIA and NPO Regulations will engage:

a. **NPO Licensing authorities:** to ensure market entry controls are prudent and effective to limit entry only to NPOs and related stakeholders who are fit and proper. On an ongoing basis, the FIC will exchange information with relevant licensing authorities to ensure only duly complying and registered entities enter the NPO space;
b. **BIPA**: In view of NPO registrations, to enhance relevant effectiveness that can enhance sound NPO entity registration at national level; and
c. **Representational and self-regulatory organisations**: Namibia's NPO sector, especially Faith Based Organisations are spread across influential representational and self-regulatory bodies. These bodies play a helpful role in enhancing compliance across the NPO sector. The FIC will need to avail training of NPOs via such bodies and roll out outreach activities with them.

7 CONCLUSION

FIA compliance assessment activities are the cornerstone of the FIC's Compliance Monitoring and Supervision framework. These activities enable the FIC to gauge risk mitigation levels at institutional and sectoral levels and thus create opportunities for corrective interventions. This then lays the foundation for timely and result driven remediation or interventions in the interests of safeguarding the integrity of the financial system.

The assessment methodology explained herein is periodically reviewed as per Section 9 of the FIA to ensure it remains relevant with the evolving AML/CFT/CPF supervisory environment.

In ensuring the effective and efficient supervision and monitoring of the FIA supervised populace, the FIC shares this FIA compliance assessment methodology to enhance

consistency and the populace's understanding of this critical supervisory component in the hope that such will contribute to enhanced engagements in as far as the execution of assessments are concerned.

8 APPROVAL

The updated FIA compliance assessment methodology as captured herein is hereby approved.

B EISEB **23 DECEMBER 2024**
DIRECTOR: FIC

ANNEXURE A

This section avails a few typical examples of observations or exceptions encountered by the FIC when conducting FIA Compliance Assessments and how such inform the eventual report findings/observations. The foundation of assurance activities is that the FIA entrusts AIs and RIs with compliance obligations, in safeguarding the integrity of our financial system. Thus, the FIC's approach is premised on selecting transactions and/or business relationships (accounts, clients), processes, operations and querying the AI or RI to demonstrate how they mitigated risks (or complied with the law) in terms of such queried or selected units.

With the consideration rating assessment findings, the level of risk mitigation effectiveness or technical compliance will largely depend on the nature and type of exceptions noted from tests, as highlighted herein above.

A. ML/TF/PF RISK ASSESSMENTS (SECTION 20A (1) and (2) & 35/NPO Regs)

*An AI/RI/NPO demonstrates whether there is a risk assessment in place: If there is none, it reflects **non-compliance** with the FIA and report findings reflects as such. Potential impact on FIC observations:*

i. *The **absence of a risk assessment** often reflects a risk-based approach is not the basis on which internal AML/CFT/CPF controls are premised;*
ii. *A **poorly crafted risk assessment report or understanding** of risk exposure equally shows that risks may have been assessed but such assessment may have challenges and would not be the ideal control guiding tool without further necessary improvements.*

The FIC has learnt that in most cases, the effective functioning of other controls as contained herein is influenced by an understanding of risk exposure at AI/RI/NPO level. Section 4.2 in Directive 01 of 2021 avails minimum considerations for a ML/TF/PF risk

assessment. Each AI/RI's/NPO risk exposure/environment will determine the nature, type and extent of factors that ought to be considered in a risk assessment.

The norm is that such risk assessment is carried out and results thereof documented. This helps with consistent application and continuity. Such report/document is then shared with the FIC. However, if there is adequate demonstration which convinces the FIC that despite such not being documented, relevant risks are known, it is accepted that a risk assessment was conducted. Thus, although it is recommended and very helpful to have it documented, in some instances such as small businesses which may be owner-operated, a demonstration of how the sole-staff member (AMLCO) understands his/her clients and duly mitigates risks could suffice.

B. FIA COMPLIANCE PROGRAM

An AI/RI demonstrates whether there is a FIA Compliance Program in place. In terms of Section 20A (4) and 35 (NPOs Regs) of the FIA, the AI/RI must develop, adopt and implement a customer acceptance policy, internal rules, programs, policies, procedures and controls as prescribed to effectively manage and mitigate risks of money laundering, financing of terrorism and proliferation (ML/TF/PF) activities. If there is none at all, it reflects non-compliance with the FIA and FIC findings would naturally point to that.

Potential impact on FIC observations:

i. *The **absence of a FIA Compliance Program** (or such relevant NPO controls) often reflects that an AI/RI has no policies, procedures and controls to mitigate ML/TF/PF Risks;*
ii. *A **poorly crafted or ineffective Program** equally shows inadequate development and adoption of policies, procedures and controls which could results in poor risk mitigation (implementation);*
iii. *A **well-crafted Program with poor implementation indications** equally results in control ineffectiveness and non-mitigation of ML/TF/PF risks.*

C. CUSTOMER DUE DILIGENCE (CDD) / KNOW YOUR CUSTOMER (KYC) (SECTIONS 21 & 22)

The KYC/CDD measures as per sections 21 and 22 mainly speak to AIs and RIs. NPOs' due diligence expectations are towards their donors, beneficiaries and such stakeholders. For NPOs therefore, reviews are based on NPO Regulations and the amended FIA section 35.

The types of services/products and level of risk exposure in an AI/RI often determines how the FIC approaches control reviews related to KYC and CDD. The following is usually the norm:

i. *The FIC requests to be availed with client financial profiles[13] (information which presents how the client is known by the institution) of selected clients/customers. By looking at the transacting activities of such clients and other factors, the FIC will, amongst others, assess whether the:*
   - *client profile has all relevant customer identification information as prescribed by the FIA and its accompanying regulations;*
   - *transacting behaviour or such other factors support the risk rating accorded to the client;*
   - *client profile was timely updated when behaviour changed, if it did, over the period reviewed.*

   Failure to demonstrate effective risk mitigation as per above factors will convince the FIC that risk management around such controls is ***inadequate or/and ineffective****.*

ii. *Usually, transactions are selected from a population of records and the AI/RI is requested to demonstrate whether the relevant CDD/KYC measures undertaken*

[13] Client profile – is a representation of the client by the AI/RI based on the information that is obtained on onboarding and during the course of the business relationship.

for such transactions (clients) are in line with client/transaction risk exposure. When the FIC is not satisfied with the demonstrated measures, observations raised would often reflect either one, or all of the below:

- ***Inadequate controls:*** *Usually refers to the adequacy in design of CDD/KYC controls;*
- ***Ineffective controls:*** *Usually refers to the actual (practical) functioning of such controls.*

Inadequate and ineffective controls observed herein often undermine the effective functioning of controls designed to comply with sections 21 and 22 of the FIA. They equally have an impact on compliance with sections 24 and 33, amongst others.

The centre of most reviews in this regard borders on whether risks, as informed by nature of services/products, transacting values, volumes etc., are in line with client financial profile at the time of transacting. For example, FIC exceptions always indicate that clients are transacting in financial values which appear outside (higher than) their stated income or transactions indicating to be outside the nature of their businesses (e.g., a non-cash or low cash intensive business transacting in large cash) as per profiles created by AIs and RIs.

D. RECORD KEEPING (SECTION 26)

It is expected that AIs/RIs demonstrate risk mitigation and thus FIA compliance by convincing the FIC that it keeps records of all:

i. CDD/KYC or identification information in the prescribed manner;
ii. transactions conducted by it; and
iii. any reports filed with the FIC.

The FIC often assesses to gain assurance that record keeping is in such a manner that it allows adequate and effective:

- *support for related controls such as monitoring (records obtained and kept in such a manner that it supports other AML/CFT/CPF measures);*
- ***reconstruction** of the transactions/activities/client profiles for Law Enforcement or competent courts of law.*

Note that although records are to be kept for five years, AIs and RIs are expected to keep such for longer when so required by relevant authorities, in particular Law Enforcement.

*With most Offsite reviews, all of the above are considered by the assessment team to arrive at an objective analysis on control **adequacy** levels. In Onsite assessment activities, such are usually assessed in terms of their **effectiveness**.*

E. ACCOUNT/TRANSACTION/CLIENT MONITORING AND SCREENING (SECTION 24) [THIS IMPACTS COMPLIANCE WITH SECTION 33]

These reviews usually commence by obtaining client profiles and listing of their transactional values and volumes. The FIC then makes assessments on whether transactional behaviour is in line with relevant client financial profiles. The risk levels of clients are often considered in the type of transactions selected (with a focus on high-risk clients/transactions). FIC reviews are premised on determining whether:

i. the nature of selected transactions is supported by relevant CDD/EDD information;

ii. unusual and suspicious transactions are flagged for further review (timely and without delay);

iii. that the transactions found to be suspicious are reported to the FIC as prescribed (timely and without delay); and

iv. client profiles were accordingly adjusted if there was change in behaviour which necessitated same; and

v. *whether VASPs screen wallets (e.g a few hops prior; monitor wallets transactions post the dealing with VASP) to duly appreciate risks associated with same and see to it that VASPs do not unduly expose themselves.*

The FIC considers AI/RI demonstrations with regard to the above factors and makes an objective assessment on whether such controls are:

vi. ***adequate:*** *usually with Offsite assessments or when speaking to the mere design and not actual functioning of the control; and*

vii. ***effective:*** *usually with Onsite assessment activities and speaks to the level of practical control effectiveness.*

F. REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES (SECTIONS 33)

Reviews of this specific control's level of effectiveness are closely linked to section 24 control reviews cited (in section E) above. One of the key objectives of AIs/RIs implementing various AML/CFT/CPF controls centres around creating a mechanism to detect red flags, alerts or unusual transactions, subject such transactions to some form of analysis in order to determine if such are suspicious for ML/TF/PF purposes.

The test entails the FIC reviewing selected transactions and querying relevant business units or management within the AI/RI to demonstrate risk mitigation as per the factors stated in section D (i - v) above. Thus, if alerts are generated and there are not grounds which explains why such were not reported as STRs or SARs, it could amount to findings which suggests shortcomings in monitoring and reporting systems. Worse, if transactions that appear outside client profiles are not detected (red flagged) and subjected to further analysis or due diligence to determine potential suspicious activities, this may point to ineffectiveness in monitoring systems designed to ensure compliance with FIA section 33.

G. FILING MANDATORY REPORTS: CASH THRESHOLD REPORTS (CTRS), ELECTRONIC FUNDS TRANSFER (EFT) REPORTS ETC. – PRIMARILY AS PER CIRCULAR 03 OF 2015 (SECTION 32 and 34)

In terms section 32 and 34 of the FIA, AIs and RIs are expected to report certain transactions to the FIC if such transactions meet certain criteria. These criteria are indicated in FIC Circular 03 of 2015.

The FIC's review entails:

i. requesting of a population of data/records that reflect transactions in a given period;

ii. selecting transactions that meet the specified reporting criteria, e.g. cash deposits exceeding NAD 99,999.99, Domestic and International Funds Transfers (EFTs & IFTs) etc.;

iii. comparing such transactions to FIC records to ascertain if:

- *there is an effective detection system or mechanism to ensure consistent reporting;*
- *same were reported to the FIC timely; and*
- *such reports are accurate, complete etc.*

Usually, from such comparisons, the FIC identifies exceptions or shortcomings and objectively determines the level of effectiveness. As with all other findings, the exceptions or specific control failures are highlighted in assessment report annexures.

H. AML/CFT/CPF AWARENESS RAISING AND TRAINING OF STAFF (SECTION 20A (6) (b))

Relevant staff members in certain positions within business units exposed to ML/TF/PF risks as well as AML compliance staff form part of the AML/CFT/CPF control framework within AIs and RIs. AIs and RIs have an obligation to ensure relevant staff members are capacitated to assist in the mitigation of such risks. Usually, through engagements with

staff who are in positions to help mitigate such risks, the FIC is able to make assessments on their understanding of the FIA and their roles and responsibilities. This review is considered with proof of efforts to enhance staff capacity such as AML/CFT/CPF training registers, training materials used to capacitate staff etc. The FIC evaluates all such demonstration of FIA compliance with capacity building obligations with actual staff members' understanding of FIA obligations to arrive at an objective observation or finding in this regard. Often, there would be proof of training having been availed but through engagements as part of the assessment or in the implementation of controls, it can become apparent that there is poor implementation which emanates from inadequate understanding.

I. INDEPENDENT REVIEW/AUDIT OF AML/CFT/CPF CONTROLS (SECTION 20A (6) (c))

Like any other risk management activity in AIs and RIs, AML/CFT/CPF controls should be subjected to assurance activities such as independent audit reviews. The objective is to avail relevant management with reasonable assurance on the effective functioning of such controls, thereby enabling interventions if need be. The compliance assessment in this regard is centered around the following:

i. *whether internal AML/CFT/CPF policy or procedure requires for such independent reviews on the relevant controls;*
ii. *whether relevant operations exposed to ML/TF/PF risks have indeed been subjected to independent reviews;*
iii. *whether the scope coverage, nature, frequency/timing and extent of such reviews were adequate to avail reasonable assurance in all relevant areas; and*
iv. *what measures, if any, management may have undertaken to enhance risk management. Such management interventions are also assessed in terms of their adequacy and effectiveness.*

The FIC requests and reviews internal audit or similar kinds of reports (if any) for specific periods. If need be, relevant stakeholders are engaged to help the FIC understand the

AI/RI's position in terms of the above (i – iii). Additionally, these independent reviews will assist when there are differences in the results of the assessments by the FIC and those of the AI/RI independent reviews.

J. REVIEWING IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS

When so required, the FIC will make use of automated thematic reviews to test risk mitigation effectiveness in this regard. The general expectations as per the FIA and PACOTPAA are documented in Directives 01 of 2022 (screening) and 01 of 2023 (TFS).

For effectiveness assessments, NPOs, IAs and Ris are expected to demonstrate that:

i. *before a business relationship is established, the prospective client/NPO stakeholder is duly identified and subjected to screening to determine if he/she is not designated by the UNSC;*
ii. *whenever the UNSC updates its various sanctions lists the entity under assessment timely (when Government Gazzettes such update) screens all clients/ stakeholders against the updated lists; and*
iii. *there are measures, in line with the FIA and PACOTPAA (see Directive 01 of 2023 and Guidance 07 of 2023) to ensure:*
    - ***timely reporting*** *of detected sanctions screen matches as required;*
    - *Asset* ***freezing without delay****; and*
    - ***prohibition*** *of availing further services.*

For Offsites and/or Technical Compliance related reviews, assessed institutions would normally be required to show that their controls, policies/procedures are duly designed to speak to the above-mentioned controls.

The FIC considers effectiveness in sanctions screening of other non-UNSC screening from a pure risk management perspective as stated in section 4.2 of Directive 01 of 2022. Some persons listed by other bodies such as OFAC may not necessarily be listed by the

UNSC but such persons may present a high TF/PF risk. It is thus essential that effective controls are implemented accordingly. In a bank, these are some observations that would be of interest to prudential authorities as such may impact correspondent banking relationships for example. Potential loss of correspondent banking relationships could have an impact on the bank's operational ability to avail certain services and depending on various factors, this could have an impact on the financial system as a whole.