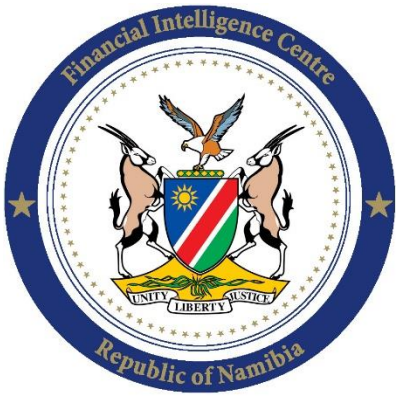

FINANCIAL INTELLIGENCE CENTRE

SECTORAL ML VULNERABILITY ASSESSMENT METHODOLOGY

First draft: January 2017

Revised: June 2018

Table of Contents

Abbreviations:

AI:	Accountable Institution.
AML/CFT/CPF:	Anti-Money Laundering, Combating the Financing of Terrorism, Combating of Proliferation Financing.
EFT:	Electronic Funds Transfer.
FATF:	Financial Action Task Force.
FIC:	Financial Intelligence Centre.
RBA:	Risk Based Approach.
RI:	Reporting Institution.
ML/TF/PF:	Money Laundering, Terrorism Financing, Proliferation Financing.
SAR:	Suspicious Activity Report.
STR:	Suspicious Transaction Report.

1. Introduction

This methodology is developed as part of the Financial Intelligence Centre's (FIC) Sectoral Vulnerability Assessment which is conducted in terms of the FATF Recommendation 1, read together with Immediate Outcome 1. A Risk Based Approach is used to guide ML/TF/PF supervisory activities of the division.

The FIC Compliance Division developed a Vulnerability Assessment Tool to determine and conclude individual sector's Vulnerability (or Risk) exposures. A Sectoral Vulnerability Assessment Questionnaire was sent out to Accountable Institutions (AI) and Reporting Institutions (RI) and the results, along with relevant considerations such as FIC understanding of sectors were used to feed the Vulnerability Assessment Tool. This document describes the methodology used in performing the Sectoral Vulnerability Assessment.

2. Objective

The Sectoral Vulnerability Assessment Methodology intends to document the approach employed by Compliance Division when:

- identifying inherent Vulnerability factors before controls are applied that could expose a sector to ML threats;
- define how the Vulnerability will be calculated, taking into account the applied risk factors;
- define the criteria for assessing consequences and assessing the likelihood of the Vulnerability, i.e. the residual Vulnerability; and
- analyse and evaluate the Vulnerabilities associated with a certain entity in the sector and the sector as a whole.

This methodology provides a detailed process followed in arriving at the sector Vulnerability rating and it further ensures uniformity, consistency and efficiency.

3. Risk Based Approach (RBA)

3.1 Vulnerability-based approach definition

A Risk-based approach involves identification of vulnerabilities, assessment, management and monitoring to determine specific focus areas based on the ML Vulnerabilities. Areas identified as highly vulnerable take priority over lower ranked areas. FATF requires Namibia, as a country to identify, assess and understand the ML and TF risks and should take actions to ensure the vulnerabilities are mitigated effectively. Based on that assessment, countries should apply a RBA to ensure that measures to prevent or mitigate impacts of risks are commensurate with the risks identified.[1]

The FIC is entrusted to, amongst others, coordinate, supervise, monitor and regulate AIs and RIs in their efforts to mitigate vulnerabilities. It is against this background that a sectoral Vulnerability assessment is conducted, based on this methodology. The Vulnerability assessment aims to streamline the FIC's supervisory and monitoring efforts going forward. The RBA will consider outcomes of the assessment and enhance the FIC's ability to prioritize its time, resources and allocate same effectively and efficiently in terms of vulnerabilities across sectors and at institutional level.

3.2 Vulnerability Profiling

Vulnerability identification: The FIC's Compliance Division identified Vulnerabilities presented by various sectors in the national financial system. The FIA, as well as the FATF Methodology at any point shall be used as guides to inform the risk and/or vulnerability identification process. The following vulnerability factors form the basis of the identification processes and methodologies:

[1] FATF Recommendation 1, Assessing risks and applying a risk-based approach

- Transaction Types: AIs or RIs in sectors with transaction types that are known to be susceptible to abuse such as conveyancing services, imports, exports, discretionary allowances contract worker remittances, and purchase and sale of foreign currency shall be accorded a higher inherent vulnerability rating.

- High Volumes of Transactions: Close attention will be paid to those AIs or RIs in sectors that deals in categories of transactions with high volumes.

- High Value Transactions: AIs or RIs in sectors that transacts in high value transactions exposes the national financial system to risk (Vulnerabilities) greater than others, thus will be rated higher.

- Method of Payments: Some payment methods are highly vulnerable to ML. For example, AIs or RIs in sectors with operations that are cash intensive exposes the national financial system to higher risks/vulnerabilities than those using other methods of payment such as EFTs.

- Geographic mapping: AIs or RIs in sectors that remit funds to and/or from, or provide services to clients from high risk jurisdictions based on high remitted values and volumes and trends of reported incidences exposes the national financial system to ML/TF/PF threats. This category also takes into account the countries listed by the FATF.

- Policies and procedures: AIs or RIs that do not have AML/CFT/CPF controls exposes the national financial sector to ML/TF/PF abuse than AIs and RIs that have effective AML/CFT/CPF controls.

- Supervisory Bodies: AIs or RIs that do not have supervisory bodies that regulate their business activities are perceived to be highly vulnerable if fit and proper assessments and similar market entry due diligence are not performed.

- Trend Analysis: The Division will collect and collate information and data from the GoAML database as well as from previous FIA Compliance Assessment reports. Information referred to in this regard will be Suspicious Transaction Reports and Activities (STRs & SARs) as well as the findings and risk exposures emanating from previous FIA Compliance Assessment Reports.

- Other secondary data: The FIC shall make use of information, news alert and statistics from other secondary sources to identify and measure vulnerabilities.

3.3 Vulnerability analysis and evaluation

The below index is used to analyze and evaluate Vulnerabilities with a view to rank same in order of priority, based on likelihood and impact. The Vulnerabilities identified will be recorded in a Vulnerability (risk) log/heat map to inform FIA Compliance Assessments.

The FIC will have to host workshops with the sectors to discuss vulnerability outcomes. The scale used is between 1 and 5 for all the sub-categories, 1 being the least vulnerability exposure and 5 being the highest exposure to risks (or higher vulnerability level).

3.3.1 Analysis of sales

The analysis of sales takes into account the percentage (%) of AIs or RIs' total sales in comparison with the total sales of the sector. AIs or RIs with higher sales percentage (%) of the sector are perceived to have higher vulnerability levels (Likelihood), hence the rating allocation (Impact) is higher than AIs or RIs with lower sales percentage (%).

Likelihood		Impact
0	10	2
11	20	3
21	40	4
41	60	5
81	100	5

Table 1: Sales Analysis

3.3.2 Geographic mapping and Clients from Foreign Jurisdictions

Geographical mapping analysis takes into consideration clients' geographical location. AIs or RIs with clients from Jurisdictions that are highly vulnerability - based on reported ML/TF/PF incidents and jurisdictions listed by the FATF as high risk (or highly vulnerable) are more like to expose the system's vulnerabilities. A rating of 5 is allocated to AIs or RIs that have more than 50% clients from these jurisdictions.

Foreign Nationals are perceived to inherently present higher risks, that may expose combatting vulnerabilities since reasonable assurance about the effectiveness of control regimes in their countries (of origin) cannot be obtained. The more an AIs or RIs has foreign clients, the higher its ML/TF/PF inherent risks. A moderate rating of 3 was allocated to AIs or RIs who have foreign clients.

	Likelihood		Impact
Namibian	0	50	5
	50	70	3
	70	100	1
Non-Namibian	0	50	1
	50	70	3
	70	100	5

Table 2: Geographical Mapping

Likelihood		Impact
Individuals	Yes	3
	No	1

Table 3: Clients Jurisdiction

3.3.3 Supervisory Bodies (or similar authority) to enter Market

This analysis compares the Vulnerability exposure of sectors that have supervisory bodies to those that do not have. The presence of supervisory bodies, and their effectiveness in driving prudential compliance enhances controls mechanisms which also positively enhance or impact combatting effectiveness. Sectors that do not have supervisory bodies are perceived to be comparatively exposed to higher risks since controls such as market entry due diligence are not performed. Conversely, AIs or RIs in sectors under prudential supervision are perceived to inherently be exposed to better market entry controls which inherently reduce ML/TF/PF vulnerabilities. A rating of 5 is allocated to AIs or RIs with no supervisory bodies.

Likelihood		Impact
Response to both questions	*Yes*	*2*
	No	*5*

Table 4: Supervisory Bodies

3.3.4 Types of clients

AIs or RIs with clients who are legal persons are relatively more vulnerable than those that have clients who are natural persons. It is easier for beneficial owners to launder through legal persons as such vehicles may be abused to conceal their identity. FIA compliance assessment observations over the years suggest that beneficial ownership information was not always duly obtained when business relationships were established. A moderate rating of 3 is allocated to AIs and RIs with a significant volume of clients who are legal persons.

	Likelihood	Impact
Legal persons e.g. Companies	Yes	3
	No	1
Individuals	Yes	1
	No	3

Table 5: Client Types

3.3.5 Vulnerability/Risk Mitigating Controls

This assessment takes into consideration implementation of controls as required by the FIA. AIs or RIs that have effective controls are perceived to have lower vulnerability levels than those that do not have effective controls in place. Based on the level of compliance observed in FIA Compliance Assessment Reports or other compliance behavioral patterns observed in the sector, AIs or RIs are rated as follows:

- Compliant: AI or RI has all controls in place, however the FIC cannot provide assurance that such controls are functioning effectively to prevent exposure of ML/TF/PF vulnerabilities. A rating of 1.5 is given to an entity that is observed to have controls in place. A rating of 1.5 represent 30% of the highest risk exposure or level of vulnerability of 5.
- Partially Compliant: AI or RI has most of the controls in place. A rating of 0.75 is given to entities observed to have most controls. A rating of 0.75 represents 15% of the highest level of vulnerability or risk exposure of 5.
- Non-compliant: If an AI or RI has no controls in place, a rating of 0 (Zero) is allocated. A rating of 0 (Zero) means that the AI's or RI's Vulnerability level remains at the highest exposure rating of 5 due to lack of controls to reduce such risk exposure or reduce vulnerability level.

Likelihood	Impact
Non-Compliant	0
Partially Compliant	0.75
Compliant	1.5

Table 6: Vulnerability Mitigants

3.3.6 Analysis by Payment Methods

Based on findings recorded in FIA compliance assessment reports and behavioral patterns observed in different sectors, some methods of payment are perceived to present higher risk exposure (or higher vulnerability levels) than others. In the risk or vulnerability assessment questionnaire, AIs and RIs were required to indicate (in percentages) the method of payment used by their clients. Below is a detailed explanation of the risk or vulnerability levels assigned for different methods of payment:

- Cash Payment: Cash remains criminals' instrument of choice to facilitate money laundering as it leaves no audit trail to suggest its true source. This form of payment is perceived to present higher risks or expose institutions to higher vulnerability levels than other forms of payment. AIs and RIs in sectors that are cash intensive were assigned a rating of 5.
- Electronic Funds Transfer (EFT): EFT is a system of transferring money from one bank account directly to another without physical notes (or coins) changing hands. The risk exposure or vulnerability level emanating from this form of payment is perceived to be moderate since these funds are within a financial institution which is perceived to have controls in place.
- Debit Cards: This form of payment allows the holder to transfer money electronically from their bank account when making a purchase. The risk or vulnerability exposure from this form of payment is perceived to be moderate since these funds are within a financial institution which is perceived to have controls in place.
- Credit Cards: Functions similar to debit cards. This form of payment allows the holder to purchase goods or services using their credit card. The risk or vulnerability level from this form of payment is perceived to be moderate since the funds are within a financial institution which is perceived to have controls in place.
- Cheque Payments: an order to a bank to pay a stated sum from the drawer's account, written on a specially printed form. The risk exposure from this form of payment is moderate since these funds are within a

financial institution which is perceived to have controls in place. Also, taking into account that cheques as a mode of payment in general are facing out within our environment (Namibia) and as such the cheques issue limit was reduced from NAD 500,000 to NAD 100,000 at the time of this assessment. The current trend suggests the public has reduced the use of cheques gradually. This mode of payment might not present a Vulnerability in future.

- Bank Financing: The extension of money from a bank to another party with the agreement that the money will be repaid. The risk exposure or potential vulnerability arising out of this form of payment lies at the repayment stage of the loans. This payment method is regarded moderate.

3.3.7 Early Settlement of Loans

This analysis has taken into consideration the period it takes for clients to settle loans and the method of payments used to settle such loans. Naturally, earlier settlement of loans enhance ML risks if the sources of such funds to settle are not known. Loans settled earlier than their settlement period, in cash, are perceived to present higher ML risks than loans settled early using other forms of payment (without cash). The table below explains the rating used. If 0-20% of loans are settled by cash, this means 80-100% of the loans are settled using other forms of payments hence the rating of 3. The same principle is applied to all levels of likelihood.

	Early Settlement by Cash	Score None Cash
Likelihood	**Impact**	**Impact**
0-20%	3	5
20-40%	3	5
40-60%	4	4
60-80%	5	3
80-100%	5	3

Table 7: Loan Settlement

3.3.8 Analysis of deposit taking

AIs that had more deposits from clients who are foreign nationals are perceived to be highly exposed to ML risks than others that have many clients from Namibia. A rating of 5 is allocated to AIs and RIs that received more than 60% of deposits from non-Namibians.

Likelihood		Score - Namibian	Score- Non Namibian
		Impact	Impact
0%	10%	1	2
11%	20%	2	3
21%	40%	3	4
41%	60%	4	5
81%	100%	5	5

Table 8: Deposits

3.3.9 Analysis of Cross Border Remittance

All AIs rendering cross border remittance services for goods and services are exposed to higher risks inherently. However, AIs rendering services of advance payments for imports are exposed to higher ML risks due to the complexity and nature of the transactions and the limited controls to verify the validity of such transactions. In order to protect the international financial system from such risks and to encourage greater compliance with controls, the FATF identifies jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international financial system. AIs and RIs rendering remittance services for advance payments of imports in excess of 40% are allocated a rating of 5.

Likelihood		Score- Other Impact	Score - Advance Payments Impact
0%	10%	1	2
11%	20%	2	3
21%	40%	3	4
41%	60%	4	5
81%	100%	5	5

Table 8: Cross Border Remittances

3.3.10 Analysis of clients from Jurisdictions listed by FATF

AIs that have clients from jurisdictions listed by FATF (calls for action) are perceived to have a higher risk exposure and a rating of 5 was given. Below is a list of countries listed by FATF as non-cooperative with international ML/TF/PF combatting efforts.[2]

Country	Score	
	Call for Action	Non-Cooperative
Democratic People's Republic of Korea (DPRK)	5	
Iran	5	
Ethiopia		3
Pakistan		3
Serbia		3
Sri Lanka		3
Syria		3
Trinidad and Tobago		3
Tunisia		3
Yemen		3

Table 9: Client Jurisdictions

[2] *FATF Public Statement. Paris, France, 29 June 2018. Jurisdiction subject to a FATF call on its members and other jurisdictions to apply countermeasures to protect the international financial system from the ongoing and substantial money laundering and financing of terrorism (ML/FT) risks.*