FINANCIAL INTELLIGENCE CENTRE

SECTORAL MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSESSMENT REPORT: SECTORS UNDER THE AML/CFT/CPF SUPERVISION OF THE FIC

First issued: September 2018
Revised and updated: July 2020

TABLE OF CONTENTS

ACRONYMS

AML	**-**	Anti-Money Laundering
AML/CFT & PF	**-**	Anti-Money Laundering/ Countering Terrorist Financing and Proliferation Financing
AI	**-**	Accountable Institution as provided in Schedule 1 of FIA
CCFAs	**-**	Customs Clearing and Forwarding Agents
CDD	**-**	Client Due Diligence
CTRs	**-**	Cash Threshold Reports
EFT	**-**	Electronic Fund Transfer
FATF	**-**	Financial Action Task Force
FIA	**-**	Financial Intelligence Act, 2012 (Act No. 13 of 2012) as amended
FIC	**-**	The Financial Intelligence Centre
ML	**-**	Money Laundering
NAMFISA	**-**	Namibia Financial Institutions Supervisory Authority (NAMFISA)
NRA	**-**	National Risk Assessment
PF	**-**	Proliferation Financing
RI	**-**	Reporting Institution as provided in Schedule 3 of the FIA
STRs	**-**	Suspicious Transaction Reports
SVA	**-**	Sectoral Vulnerability Assessment
TF	**-**	Terrorist Financing

SECTION A: INTRODUCTION

1. Introduction

As per Recommendation 1 of the Financial Action Task Force[1] (FATF), Namibia as a jurisdiction needs to conduct a National Risk Assessment (NRA). The outcomes from such NRA activity should then guide national efforts to combat Money Laundering, Terrorism and Proliferation Financing activities.

The FIC, being Namibia's agency charged with coordinating the NRA activity has completed Sectoral Risk Assessments (SRAs). These assessments considered areas within the various sectors which are vulnerable (or susceptible) to Money Laundering activities along with relevant threats that may undermine such vulnerabilities.

Namibia conducted her first NRA exercise in 2012. Amongst others, the 2012 NRA had certain gaps, such as limited in depth analysis of sectoral vulnerabilities. In 2015/16, the supervisory bodies[2] coordinated the execution of sectoral risk assessments in sectors under their supervision. Such yielded these sectoral risk assessment reports. In terms of FATF Recommendation 1 and international best practices, risk assessments are by their nature living documents that are updated as material factors change or any other need arises which necessitates revision. For this reason, this report was first compiled in 2018 and again updated in certain areas in mid-2020.

The national risk assessment exercise also commenced in 2020, with the World Bank training the entire NRA project team the first quarter of the year.

All sectors which are not under the AML/CFT/CPF supervision of NAMFISA are supervised by the FIC. This report presents observations and analysis on the ML

[1] The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

[2] FIC and the non-banking financial supervisory body (NAMFISA)

vulnerability of all sectors under the supervision of the FIC, except for the Non-Profit Organisations (NPOs). The NPOs' sectoral risk assessment was conducted separately and outcomes thereof contained in a separate report. It is advised that this report be considered along with the sectoral report on NPOs.

2. Objectives

2.1 Objectives of vulnerability assessments

The objectives of the sectoral vulnerability assessments were to:

a. identify ML inherent vulnerabilities within the sector;
b. assess the significance and impact of such vulnerabilities;
c. assess the effectiveness of relevant mitigation controls to understand residual vulnerability levels;
d. rank the products and services in terms of their vulnerability to ML;
e. rank the entities in the sectors based on the assessed vulnerability; and
f. provide a basis and rationale that informs FIA compliance supervision and monitoring activities in terms of the risk-based approach.

2.2 Objective of ML threat assessments

The primary objective is to identify the common predicate offences (threats/crimes) that generate illicit proceeds, understand the scale of such proceeds as well as the methods and trends employed in laundering same. Overall, such understanding should help stakeholders identify the trends, methodologies used to launder.

3. Methodology

Generally, risk assessment methodologies are premised on the understanding that a risk profile or position is arrived at by:

a. analyzing the level of relevant **Vulnerabilities**; and

b. considering such with potential and actual **Threats** *(Risk = Threats + Vulnerabilities)*.

This section outlines the methodology followed in arriving at the ML vulnerability profile of the Lending sector and its institutions.

Generally, the nature and characteristics of products and services contribute to their attractiveness to launderers. Given this, the vulnerability assessments considered areas within the various sectors which can be susceptible to ML abuse. Such areas include, but are not limited to:

i. the nature of products and services;
ii. types of clients using such;
iii. delivery channels of such products and services;
iv. control frameworks at institutional and sectoral levels; and
v. effectiveness of supervision etc.

On the other hand, threats speak to factors that can undermine or take advantage of such vulnerabilities (shortcomings) within the control frameworks of institutions. For example, the number of predicate offences that have manifested through certain products/services and abused delivery channels could give an indication of the level of actual vulnerability and thus risk exposure.

The methodology was also aligned with several other relevant guidance mechanisms including:

i. The FATF 40 Recommendations, the Methodology used for assessing compliance with international AML/CFT/CPF standards within the FATF framework; and
ii. Money Laundering and Terrorist Financing Risk Assessment Strategies paper by the FATF and the Guidance note on ML/TF risk assessments.

Having regard to all the guidance form the above, the methodology adopted was premised on the following:

a. drafting of the Sectoral Vulnerability Assessment (SVA) methodology which guides all activities;
b. development of the SVA tool used in capturing, processing and analyzing data;
c. questionnaires send to the sectors seeking specific data;
d. capturing, processing and analyzing such data to produce valuable information;
e. analyzing such information within the context of sectoral ML vulnerability to understand vulnerability levels;
f. reviewing of threat elements along with other relevant factors; and
g. drafting of a report summarizing major observations and analysis.

This assessment initially covered the period leading up to December 2017 and will be revised on an ad-hoc basis, as and when the need arises.

3.1 Technical approach

ML threat assessment was undertaken as per the World Bank assessment previously employed in the 2012 NRA exercise. For the SVA, a SVA technical framework was developed by the FIC to guide the technical process of unpacking sectoral vulnerabilities. In summary, the following considerations were key in the analysis of inherent factors along with obtained data to arrive at conclusions on vulnerability profiles:

a. the vulnerability assessment tool rates structural indicators from low to high, based on the certain data; and
b. the scale used was between 1 to 5 for all the sub-categories with 1 showing the least exposure and 5 indicating the highest level of exposure. See Table 1 below:

Vulnerability Assessment Score		
Vulnerability Score	**Color**	**Scale**
High		4.01 - 5
Medium-High		3.01 - 4
Medium		2.01 - 3
Low-Medium		1.01 - 2
Low		0.01 - 1

Table 1: Vulnerability Assessment Scores

4. Overall assessment outcomes

Arriving at a risk position is informed by the level of threats and sectoral vulnerabilities. This assessment found the sectoral vulnerability to be **Medium (2.82)** while threats were rated as **High**, thus arriving at the overall level of **Medium High**. The table below summarizes the consolidation of both threat and vulnerability assessment outcomes.

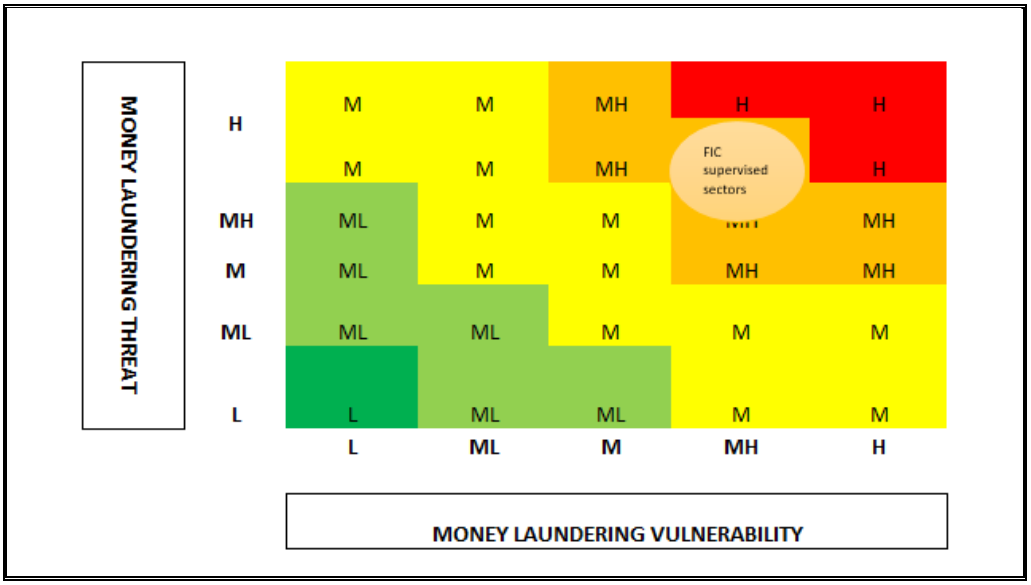

Table 2 Overall risk position of sectors under FIC supervision

4.1 ML threat

For the sectors under FIC supervision, the overall ML threat emanating from predicate offences and cross border threats is rated **High**.

4.2 Sectoral vulnerability

The table below presents a summary of the SVA results of all the sectors. An in-depth account of the provisions measuring up to the individual SVA ratings are discussed in Section D of this report.

Sector	Vulnerability Rating
Legal Practitioners	2.18
Lending Sector	2.18
Customs Clearing and Forwarding Agents	3.88
Auctioneering Sector	3.45
Casino Sector	3.22
Real Estate Agencies Sector	2.13
Banking Sector	3.78
Motor Vehicle Dealership Sector	3.38
ADLAS Sector	2.18
Accountants and Auditors	1.86
Overall sectoral vulnerability score	**2.82**

Table 3: Sectors overall Vulnerability Ratings

Sectors such as Banking, Customs Clearing and Motor Vehicle Dealership sectors were found to carry the highest ML vulnerability levels. Below are some of the key factors that informed such findings:

a. *Customs Clearing and Forwarding Agents*: major control weaknesses including:
   i. inadequate due diligence by financial institutions,
   ii. manipulation of the declaration process at customs to evade taxes, duties etc, and
   iii. lack of a national transaction reconciliation framework which can reconcile/compare what has been declared at customs, with actual remittances at financial institutions;

b. *Banking sector:* Almost all transactions nationally, from all sectors pass through the banking sector. Banking sectors have had comparatively more matured AML compliance frameworks. Despite this, the huge volumes of clients and transactions in the sector escalate the risks as control frameworks in banks are under strain to effectively combat ML. Control weaknesses in all other sectors also expose the banks (for example, the abuse of trust accounts by legal practitioners, irregular/fraudulent customs related transactions etc.;

c. *Motor Vehicle Dealerships:* market entry to this sector does not include any reviews on beneficial ownership assessments in terms of fitness and propriety. Stakeholders merely need to register legal entities or trade as a 'sole traders' and start trading in motor vehicles. There is no prudential supervisory body in place. For AML/CFT purposes however, the sector is supervised by the FIC. From the FIC's supervisory work, and as documented in the sectoral risk assessments, there is room for improvement in the AML controls of motor vehicle dealers.

5. Challenges Observed

The intended completion date of the SVA, as per approved Project Charter was envisaged for 30 April 2018. The project activities were not completed timely. This is primarily because additional activities were added to the planned activities, thus inherently extending anticipated completion date.

The *Modus Operandi* entailed extracting contact details from the FIC database for all registered AIs. Such registration contact details guided the FIC in terms of known entities that were engaged for data gathering purposes and thus partake in the assessment. Below is a presentation of major challenges worth noting and how they were managed:

a) Due to the FIC database not being updated with all relevant contact details, it became challenging to obtain the relevant contact addresses of respective entities and persons who had to be engaged for this exercise. Other measures of obtaining contact details had to be employed and thus timelines were affected;

b) The knock-on effect of failures in one phase: The unavailability of contact detail information due to poor record keeping naturally contributed to the delay in completion of other planned activities such as disseminating of questionnaires to the sectors, analyzing responses and collating or making sense of such analysis within the planned timelines;

c) Data and record keeping within the domains of Law Enforcement Authorities (LEAs) is not kept in a manner that easily supports the standards set for executing AML/CFT risk assessments. For example, LEAs would have record of all cases

registered with minimal information on sectors from financial crimes may have emanated;

d) The ability of the regulated populace to understand and respond to the request for data/information effectively and timely was a challenge. This could be partly attributed to the fact that sectors were not adequately informed. In hindsight, the FIC has noted that it failed to conduct information briefing sessions or similar activities to enhance stakeholder understanding of key expectations, enabling the contextualization of its intent and importance of the exercise. The team had to individually engage and assist entities who struggled to understand and avail information;

e) One of the challenges was with the Information Technology (IT) facilities to enable an automated and thus timely capturing and analysis of the results received from the sectors. The planning was premised on the expectation that a specific IT facility would be used to source and analyze data, thus resulting in speedy completion of the data gathering and analysis phases (key phases of the project). Upon implementation, it was realized that such facility was not suitable, and the gathering and analysis had to be done manually;

f) The late submission of completed questionnaires delayed the timely completion of the project. Follow-ups and new deadlines had to be agreed with the participants; and

g) Although project timelines were provided for in the Project Charter, the time required for the project was underestimated (not realistic) as it did not take into consideration of some of the above constraints.

SECTION B: ML THREAT ASSESSMENTS

6. Objectives of the threat assessment

The primary objective is to identify the common predicate offences (threats/crimes) that generate illicit proceeds, understand the scale of such proceeds as well as the methods and trends employed in laundering same. Generally, the essential outcome of this assessment is to understand how ML threats expose institutional and sectoral vulnerabilities (ML methodologies and trends) in the AML/CFT/CPF framework. Factors such as poor record keeping within combatting authorities limit the ability to have sufficiently reliable data. The threat assessment herein thus has limitations primarily caused by data limitations.

6.1. ML threat rating

For the sectors under FIC supervision, the overall ML threat emanating from predicate offences and cross border threats is rated High. In the 2012 NRA exercise, the overall national threat element was rated as **Medium High**. Amongst various considerations, the following were key considerations which necessitated an escalation of threats from **Medium High** at national level in 2012 to **High** in 2018 for the sectors under FIC supervision:

6.1.1 *Escalation in the volume and significance of ML cases brought before court*

As per the NRA report of 2012, Namibia did not have any cases wherein ML was successfully prosecuted. The few successful prosecutions recorded may thus reflect progressive maturity in the AML/CFT/CPF framework. In recent years, significant ML threats materialized, leading to actual predicate offences which were investigated by AML/CFT/CPF authorities and brought before court. Some major cases include *the Customs Clearing Agency case in which over NAD 3 billion (USD 300 million) was fraudulently remitted; the fraudulent Value Added Tax refund case in which the state was defrauded of funds in excess of over NAD 13 million; the SME Bank case in which a bank may have been defrauded of depositor's funds in excess of NAD 240 million resulting in*

the eventual liquidation of the state owned bank[3] (these cases are discussed in detail herein).

6.1.2 *Growth in the threat of cross border remittances*

Generally, AML/CFT/CPF authorities has seen an increase in predicate offences committed by exploiting cross border remittance vulnerabilities in certain sectors. The major case studies cited herein reflect a cross border remittance element to it.

6.1.3 *AML/CFT/CPF resource constraints*

The natural consequence of resource constraints is reflected in the very low volumes of ML investigations yielding prosecutions and convictions locally. Resource constraints also impact the courts as they are often overwhelmed with the volume of case at hand. Naturally, the finalization of ML investigations, prosecution and judicial process are negatively impacted. At investigative and prosecutorial level, the lack of specialization in identifying, tracing of proceeds, performing financial investigations and bringing ML cases to court is cited as a major challenge. It therefore goes without saying that generally, there are no factors indicating that finalization of ML investigations and prosecutions have not improved since the 2012 NRA observations, despite the 2012 NRA outcomes recommending that the county improve its resource allocation to the AML/CFT/CPF framework.

6.2. Understanding ML predicate offences

6.2.1. ML investigations, prosecutions and convictions: 2015-2018[4]

Year	2015	2016	2017	2018
Number of investigations with an ML component	72	119	80	100
Number of ML prosecutions initiated	07	10	12	14
Number of convictions for ML	02	0	01	01

Table 4 record of investigations and prosecutions

[3] Factors around the so-called fishrot scandal in which the widespread corruption is alleged are still sketchy and the case is being analysed as part of the 2020 NRA revision. It will be assessed as a threat in such revision.
[4] Source: Namibia Police

Below are crime statistics which highlight the volume of cases reported for various crimes in the period assessed:

CRIME DESCRIPTION[5]	2012	2013	2014	2015	2016	2017	2018
Income Tax	2	1	1	1	2	2	1
Corruption[6]	62	52	54	52	49	105	93
Fraud: General	2,177	1,935	2,062	2,177	2,118	2,049	2,149
Fraud: Forgery and uttering	255	236	339	279	263	297	289
Fraud: All other frauds, forgeries, conversions or embezzlements	18	39	10	29	13	20	6
Nature Conservation Ordinance (Poaching)	267	356	228	351	477	359	644
Prevention of counterfeiting of currency Act	36	58	28	46	36	68	49
Trafficking in persons	-	-	-	-	-	5	15
Illegal trafficking in diamonds	-	2	-	1	-	1	-
Illegal possession of diamonds	10	4	1	4	1	9	35
Stock Theft	2,542	2,343	2,386	2,446	2,578	2,705	2,791
Theft of motor vehicle	290	298	314	392	440	383	367
TOTAL	**5,659**	**5,324**	**5,423**	**5,778**	**5,977**	**6,003**	**6,439**

Table 5: Crime statistics for the years 2012 - 2018

The assessment, with regard to data at hand revealed that crimes such as **Tax Evasion, Corruption and Fraud** are some of the most prevalent predicate offences for ML and the resultant ML threat was rated **High** for each of these offences. In terms of the volumes of predicate offences within the ambits of LEAs, cases of fraud are largely the most reported and investigated cases nationally. Apart from financial values related to potential tax evasion, the project team experienced challenges obtaining financial values related to cases of fraud and corruption. This was highlighted as a major challenge in the 2012 NRA project. Record keeping within LEAs currently does not enable ease with which the country can financially quantify the significance of these crimes, as done with tax evasion in this report.

The write up below avails a breakdown of these three major predicate offences and factors that informed their ML threat rating herein.

[5] Source: Namibian Police

[6] These are the few cases of white-collar crimes under investigation by the Namibian Police, with a corruption element to it. The Anti-Corruption Commission of Namibia, as the entity charged with investigating corruption, primarily investigates all corruption related matters locally. These statistics should thus be viewed with the section 6.2.1(b) below which speaks to corruption.

a. Tax evasion

Despite a commendable policy framework and general tax evasion enforcement measures, there is room for improvement and the tax evasion threat was thus rated **High**. The reason for the high rating was a result of the inadequate mechanisms for the monitoring and enforcement of compliance with tax obligations. The examples cited herein relating to tax control weaknesses within cross border remittances and the Customs and Excise framework further contribute to the challenges which undermine the effectiveness of Namibia's tax collection framework.

i. Domestic tax evasion

The table below[7] shows the volume of STRs disclosed by the FIC to various LEAs and competent authorities. Disclosures to the Ministry of Finance are mainly indicative of potential tax evasion threats, mainly domestic. As far as intelligence analysis is concerned within the FIU, tax evasion threats in the period assessed have largely been the primary source of potential ML.

Year	*2009*	*2010*	*2011*	*2012*	*2013*	*2014*	*2015*	*2016*	*2017*	*2018*	*Total*
Anti-Corruption Commision	4	7	6	27	6	8	7	7	5	10	87
Ministry of Finance	12	28	40	41	24	82	38	43	51	119	478
Namibian Police Force	19	36	55	68	23	48	38	47	16	49	399
Office of the Prosecutor General	-	1	31	6	4	9	15	32	31	13	142
Foreign FIUs	1	3	16	18	15	6	-	-	5	6	70
Others	2	8	4	8	9	18	22	9	31	16	127
Total	38	83	152	168	81	171	120	138	139	213	1 303

Table 6 Volume of STRs disseminated to various LEAs and competent authorities

[7] FIC Annual Report, 2018

The table below shows data obtained from the Ministry of Finance reflecting potential tax evasion cases investigated, relevant tax amounts raised and collected in such regard:

SUMMARY OF POTENTIAL TAX EVASION AND AMOUNTS RAISED FOR SUCH			
Date	**Possible Offences**	**Tax amounts raised (NAD)**	**Amounts Collected (NAD)**
2014	Tax Evasion & ML	1,327,958.90	1,160,812.23
2016		786,477,052.20	25,035,796.57
2017		13,161,929.64	327,696.37
2018		1,527,318.44	5,432,577.34
	Estimated Totals:	**802,494,259.18**	**31,956,882.51**

Table 7 Summary of potential tax evasion and amounts raised

ii. Cross border tax evasion and ML

Case study 1

A case involving a Customs Clearing and Forwarding Agency (CCFA) and mainly locally based firms operated by Chinese nationals was subjected to an LEA investigation. The case is still before court. The investigation observed that most, if not all invoices involved with this clearing services provider do not appear legitimate. The following were major characteristics of such transactions:

- *they lack the basic characteristics of a tax invoice such as proper address and contact details, poor description of goods etc.;*
- *in most invoices reviewed, over 90% of the invoiced amount is allocated to line items such as Transport, Cartage and Storage costs etc. Usually, only about 5 – 10% of the total invoice value is indicated as Free on Board (FOB) value.*

The reduced FOB value is the actual value of goods, on which import VAT, Duties etc., are levied as per the questionable invoices observed. Another feature, which was immediately questioned by customs officials upon presentation of this case study - is the fact that substantially bigger containers are recorded to have been used, which may seem inconsistent with the significantly smaller size/value of goods declared (FOB). Large containers could be used to justify the higher costs attributed to transport and such other costs.

Investigations indicated that by April 2017, remittances in excess of USD 300 million (over NAD 3 billion) were facilitated in such irregular manner. The difference (of USD200 million or NAD 2.7 million) between the invoices presented to the bank (USD 280 million or NAD 2.9 billion) for forex remittances and those presented to Customs (USD 20 million or NAD 210 293 896), may indicate misrepresentation by the involved CCFA, and the respective Namibian importers to the bank in order to irregularly remit funds offshore. The SAD500 customs declaration documents did not always seem to have been duly declared at Customs and Excise Authorities. Also, large volumes of cash deposits (NAD 3 337 860 481 by April 2017) appeared potentially non-commensurate with the nature, type and size of the importers' nature of businesses. In addition, the analysis of the remittances by each importer - when compared to available financial statement information indicated a significant understatement of purchases, further advancing potential cross border tax evasion.

Continuation of Case study 1 ….

A typical irregular invoice used by the CCFA to advance the fraud and tax evasion herein looked as follows:

Item Type	***USD***
Value of goods (FOB)	*2,500.00*
Freight charges	*200,000.00*
Haulage charges	*110,000.00*
Storage	*180,000.00*
Handling	*165,000.00*
Total invoice value:	***657,500.00***

Case study 2

A local based entity specializing in the importing and retailing of used vehicles was suspected to have been involved in potential tax evasion and ML. The firm was registered as an importer, and thus declared its imports without the use of a customs clearing and forwarding agent. For all cross-border remittances presented at financial institutions, only "draft" Bills of Ladings and Invoices were attached, without any SAD500/import customs declarations documents attached. In many instances, the invoice numbers appear to have been reused, for different transactions, across different financial periods. Most of its imports are from the United Arab Emirates (UAE). We strongly suspect that it is conducting transactions which have indicators of capital flight, potential tax evasion and ML. The norm is that actual payments for invoices are always more than the sum of all invoices attached.

Below are two real examples, which also suggests that there appears to be poor due diligence at involved financial institutions:

- *Total amount remitted to the UAE was USD 184,860.00, while the total invoices add up to USD 92,360.00 only; and*
- *Total amount remitted to the UAE was USD 199,290.00, while the total invoices add up to USD 67,500.00 only.*

The company remitted a total of USD 90,676,945.28 in the 2014 calendar year alone. This was spread over 65 transactions and seem out of line with expected industry revenue norms locally.

b. Corruption

Corruption is primarily investigated by the Anti-Corruption Commission (ACC). Whilst acknowledging notable efforts made in combatting corruption through the establishment of dedicated bodies such as the ACC, the general anti-corruption controls within various sectors (at institutional levels) of the economy contribute to the overall growth in the number of corruption cases. In the same vein, the slow pace at which corruption cases are investigated and brought before court for finalisation presents one of the biggest challenges in combatting corruption. Essentially, resource constraints significantly hamper the effectiveness of the ACC as investigating officers are often overwhelmed with work. These two factors, in the main, are regarded as escalating the threat of corruption to a **High** rating. Below is an overall view of cases submitted to the Office of the Prosecutor General (OPG) by the ACC since inception[8]:

- *The ACC has submitted 587 cases to the OPG;*
- *240 cases (41%) are still in court and have not been finalised, some dating back as far as 2007;*
- *118 (66%) of those that were finalised resulted in convictions;*
- *60 (34%) of those that were finalised resulted in acquittals;*
- *In 86 (15%) of the cases the Prosecutor General declined to prosecute;*
- *14 cases (3%) in total are currently with the Commission in order to comply with further instructions;*
- *50 cases (9%) are still awaiting a decision by the Prosecutor-General;*
- *9 cases were withdrawn;*
- *5 cases were transferred to the Namibian Police; and*
- *In 5 cases the accused passed away.*

In the 2017/18 financial year in particular, the ACC received 325 complaints representing a decrease of 20 cases from the 345 complaints received during the 2016/17 financial year. In 2017/18, 156 (48%) of the 325 complaints received were earmarked for investigation by

[8] ACC 2017/2018 Annual Report

the ACC, compared to 168 cases during the previous financial year. The complaints received by the ACC were both corruption and non-corruption related. Approximately half the complaints received by the ACC over the three years leading to 2017/18 were non-corruption related and were referred to the relevant government authorities for their action. The quality and amount of relevant information of the corruption complaint received determines whether the case can be pursued. The majority of non-pursuable corruption complaints were due to insufficient, vague or unsubstantiated information provided.

The case study cited below, whilst reflecting effective investigation which uncovered the scam and led to arrests shows how fraud and corruption resulted in losses incurred by the state.

Case study 3

Four foreign nationals came to Namibia on visitor permits. Whilst in Namibia, they made various purchases on which VAT was charged on the goods. As per the VAT Act, foreign nationals may claim the VAT incurred on certain goods and services upon their exiting from Namibia. The Ministry of Finance has appointed agencies which facilitate the processing of VAT refunds. The said foreign nationals colluded with employees of the local agency to fabricate illicit, and inflated invoices and submit fraudulent VAT refund claims. These refunds were made in the form of either cheque payments or redeemable vouchers. These vouchers were redeemed at various money remitters (ADLAs) while significant amounts were also sent to one foreign jurisdiction for the benefit of the said foreigners involved in the fraud.

Significant deposits (cheques and cash) were made into personal and business accounts, resulting in regular large Electronic Funds Transfers (EFTs) and cash withdrawals received by this group of foreign individuals and entities. The bank accounts of one of the involved entities was fairly recently opened, with very limited transactional activities on such accounts, except for transactions relating to the fraudulent VAT claims. Some indicators are that the business accounts involved showed no resemblance to expected business transacting activities and the main source of income comprised significant VAT refunds and subsequently followed by EFTs, cash withdrawals and Point of sale (POS) transactions on seemingly private expenditures. The bank accounts were held at three different local banks. Over NAD 13 million was lost by the state.

c. Fraud

As mentioned above, statistics regarding the total amount of illicit proceeds involved in all cases reported and investigated are not currently being kept as required. The absence of these statistics amounted to cases investigated by LEAs not having any monetary values assigned to them. Owing to this, a more accurate total of illicit proceeds related to many predicate offences including fraud could not be established. The high volume of fraudulent cases within the investigations of LEAs, relative to the volumes of other economic crimes as per Table 5 above mainly informed the **High** threat rating. Below is a case study which summarizes potential fraud and subsequent cross border money laundering at a large scale, potentially leading to the liquidation of the Small and Medium Enterprises (SME) Bank in Namibia.

Case study 4

The case is currently before court, what is known is that large funds were remitted outside Namibia as investments and such never returned, consequently adding to the cash flow challenges the bank had. The SME Bank was primarily established to support and stimulate SMEs through the provision of business loans locally. The Namibian government sought foreign investors, who would become minority shareholders. The minority shareholders, as part of the agreement with the government were to be represented on the board and would bring in the necessary expertise to run the affairs of the bank. The executive management of the bank, including the Chief Executive Officer (CEO), was primarily made up of the foreign personnel brought in to represent the minority shareholders.

In early 2017, the Bank of Namibia intervened in the banking operations of the SME Bank and successfully placed the bank under provisional liquidation as it had cash flow challenges and was at risk of failing to honour deposits, amongst other challenges. Liquidators have for the last few years been liquidating the bank, with much efforts spend trying to recover the bank's funds from the minority shareholders and their associates.

As part of their liquidation efforts in terms of the Companies Act, the liquidators, as per their court papers, are convinced that the minority shareholders and the management may have defrauded the bank, leading to the cash flow challenges the bank experienced. In their claim, the liquidators state that between 11 October 2012 and 29 April 2015, an amount of NAD 97.1 million was remitted to South African recipients. Again, an amount of NAD 53.5 million was also transferred to South Africa between 30 April 2015 and 1 September 2015, followed by another transfer of NAD 97.5 million to South African recipients between 1 September 2015 and 17 January 2017. All these transactions were allegedly made at the time when one of the minority shareholders was the deputy chairman of the bank's board, who knew or instructed the executive management to execute such transfers. This is raised in the court papers wherein the liquidators are asking the court to declare the deputy chairman liable for the debts of the SME Bank in terms of Section 430 of the Companies Act.

Continuation of Case study 4 …

Potential round tripping of funds transferred from the SME Bank

A local company called Omulunga Capital Investments CC (OCI), owned by a person who is alleged to be closely linked to the minority shareholders was placed under provisional liquidation by the High Court for money illegally spirited out of the SME Bank. The first claim against OCI is for an unpaid loan of NAD 5.5 million at 20% interest per year, for which SME Bank liquidators could not find any documents confirming a written loan agreement. The liquidators further state that the owner of OCI was one of the recipients of the NAD 79.8 million siphoned from the SME Bank and paid over to a South African-based company and so-called "money laundering machine" known as Asset Movement and Financial Services CC (AMFS). Funds would usually return from AMFS back to OCI in Namibia. All payments made by AMFS to OCI were initiated from the former SME Bank CEO's office, who indicated the purpose of the transfers as "investments" in Mamepe Capital Asset Managers. Mamepe Capital Asset Managers is the black empowerment financial services company in South Africa headed by Kotane Mauwana. None of the money was paid over to Mamepe though, and the liquidators say it was simply stolen.

The liquidators found that although former SME Bank financial manager did not sign payment instructions to AMFS, he is the next of kin of the owner of OCI and they had the same address in Windhoek.

The link with Dubai

A Dubai-based company, known as Aulion Global Trading DMCC, a precious metals trading company, issued an invoice of NAD 64.5 million to OCI on 21 January 2016. Court records further show that one day before the owner of OCI applied for his first account with the SME Bank – on 26 January 2016 – an employee of Howie Baker of Pivot Capital (Pty) Ltd had instructed the sole director of AMFS, to transfer NAD 7.1 million to an SME Bank account held at a local bank, with a payment instruction referenced as 'Omulunga Capital Investments'.

On 27 January 2016 AMFS transferred the NAD 7.1 million to the SME Bank's account held at a local banking institution. This amount was later transferred to OCI's account held in the SME Bank as per email instruction from the owner of OCI.

Further payments followed the same route – money transferred from AMFS to SME Bank accounts held at various local banks – and then laundered through OCI's bank accounts held at SME Bank and transferred on to Aulion Global Trading DMCC in Dubai. The total payments made by AMFS amounted to NAD 26.2 million and a total of NAD 25.7 million was paid over to Aulion Global Trading DMCC.

In a matter of weeks in June 2016, about NAD 4.6 million was also paid to Aulion Global "after being round-tripped" through four different accounts held by OCI at the SME Bank and a local bank, state the liquidators. In July that year, another NAD 4.5 million went via a local bank account into one of OCI's SME Bank accounts, this time with the source of the funds stated as Aulion Global. A NAD 4.4 million remained in OCI's SME Bank account until 7 September that year, when NAD 4.2 million of it was again paid over to Aulion Global. This case once more demonstrates how potential fraud, as a predicate offence, resulted in proceeds being laundered through cross border remittances and laundered through the banking system.

The eventual closure of the bank, resulting in depositors losing their money and complete failure of a SME funding institution again shows the severe impact ML can have on the financial sector and country at large.

6.2.2. Geographic risk (cross border remittances)

Namibia largely relies on importation of goods and services to augment her domestic production. The role of CCFAs in import declarations and remittances is essential. CCFAs with clients from jurisdictions that are high risk, based on reported incidents and jurisdictions listed by the FATF as high risk are more inherently vulnerable. [9]This study found that some CCFAs receive or remit funds to some jurisdictions listed by the FATF as non-cooperating countries as well as other jurisdictions identified as high risk for capital flight and tax evasion in Namibia. The People's Republic of China has also been added to this list as it was found to expose Namibia to tax evasion and ML risks. The Bank of Namibia indicated that the total amounts of money remitted from Namibia to these jurisdictions including The People's Republic of China for the 2017 and 2018 financial years are as follows:

No	Outflow to Countrry	2017 (NAD)	2018 (NAD)
1	The Bahamas	28,864,317.04	71,148,414.17
2	Botswana	3,153,064,694.54	2,575,271,267.29
3	Cambondia	-	47,903.57
4	Ethiopia	1,722,672.01	5,101,556.36
5	Ghana	4,537,168.62	4,214,923.02
6	Pakistan	956,528.66	2,542,051.77
7	Panama	1,315,565,861.35	155,691,374.33
8	Sri Lanka	455,472.12	298,931.29
9	Syria	-	-
10	Trinidad and Tobago	25,323.08	-
11	Tunisia	5,440,725.65	5,323,686.48
12	Yemen	6,335.05	-
13	The Peoples Republic of China	695,004,159.36	2,162,401,195.59

Table 8 Remittances to High-risk and other monitored jurisdictions

[9] High-risk and other monitored jurisdictions: The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in two FATF public documents that are issued three times a year. The FATF's process to publicly list countries with weak AML/CFT regimes has proved effective (click here for more information about this process). As of October 2018, the FATF has reviewed over 80 countries and publicly identified 68 of them. Of these 68, 55 have since made the necessary reforms to address their AML/CFT weaknesses and have been removed from the process (see also, an overview of the jurisdictions currently identified in this process).

6.2.3. Sectoral origins of ML threats

	BANKING SECTOR													
	Private Banking (No. 1)	Retail deposits (deposits by natural persons)	Deposits of legal persons	Micro-credit products (small credits/loans availed by banks to persons)	Credit products for retail customers or natural persons	Credidt products for small & medium sized businesses	Credit products for large businesses	Trade finance (No. 2)	Current accounts (No. 3)	Wire transfers: Locally & within the CMA	Wire transfers: Internationally (Outside the CMA)	Electronic banking	Negotiatble instruments (Chequest etc, promissory notes) (No. 4)	Trust & Asset Management Services (No. 5)
2018	12	137	144	10	11	3	0	39	186	31	21	77	20	3
2017	11	111	96	5	6	0	0	21	125	18	4	37	54	5
2016	3	33	348	3	4	0	3	26	92	2	35	20	45	12
2015	0	51	200	3	8	1	3	24	60	2	11	20	46	9

1. Private Banking (Exclusive clients or those earning over N$ 800k annually)
2. In this context, trade finance could include Letters of Credit (LCs), export finance and credit agencies, receivables and invoice finance, as well as bank guarantees. It is also known as supply chain and export finance
3. Current acocunts are your normal client accounts (cheque/savings or similar types of accounts)
4. Negotiable instruments are documents which promise payment to the assignee (the person whom it is assigned to/given to) or a specified person.
5. Includes operations related to custodial services and share certificates (nominee shareholding) etc., as well as drafting and reviewing of trust deeds, management of assets in trust

Table 9 STR reporting behaviour of the banking sector

Given that data within LEAs is not kept in a manner that enables tracing of cases to the relevant sectors and products/services abused to advance ML, this assessment relied primarily on STR data[10] within the domains of the FIC.

Most banks are affiliates or subsidiaries of international financial institutions. For this reason, most of them had implemented AML/CFT/CPF controls before the FIA came into operation. When compared to other sectors, the banks' AML/CFT/CPF control systems have thus progressively matured over the years. Such matured systems are relatively more effective in helping to detect and report the STRs. Amongst other factors, this explains why the banks generally report the highest volume of STRs to the FIC.

The ML threat in the banking sector was assessed to be relatively **High**. Inherently, the banking sector is exposed to the risk of dealing with proceeds from several sectors which make use of banking services. Almost all sectors make use of the banking system and the sector is naturally one of the few that deals in the highest financial values and volumes nationally. The STR reporting behaviour also

[10] STRs analysed by the FIC and case files opened and escalated for further review by relevant competent authorities. This excludes STRs not subjected to FIC analysis and diligence.

tends to suggest the specific baking products and services most susceptible to ML threats, with services such as retail deposits and deposits of legal persons potentially being abused more than other services.

In terms of ML threats to other sectors, the DNFBPs' sector[11] appear to be exposed to relatively medium to high ML threat levels. Some key take-aways from sectoral abuse are as follows:

- *indications illustrating the vulnerability of the casino/gambling industry whereby large amounts of cash have been noted in reports received by the FIC. These reports indicated the ability to "place" money at the cashiers within a gambling institution by loading the corresponding value onto one of the gaming instruments (such as loyalty cards or MVG cards). The trend identified indicated that funds would be redeemed after limited gambling activity either in cash (but for different notes) or to be transferred to a bank account or even to another gambling institution (locally or abroad) affiliated to the gambling institution;*

- *when Namibia's property market was experiencing a boom a few years ago, it also attracted investors from various jurisdictions to invest in and own property. The extent to which these transactions may involve proceeds of crime could not be assessed, but with the existence of transnational crime syndicates operating in the region and the vulnerabilities identified within the sector suggests that a notable threat exists within the real estate sector.*

Below are various tables presenting the STR reporting behaviour of several sectors. These are STRs which had undergone FIC analysis and were escalated for further investigations by LEAs.

[11] Comprising, amongst others, legal practitioners, auctioneers, accountants, the real estate sector, casinos, dealers in precious metal and stones and the motor vehicles dealers.

	DNFBPS: REAL ESTATE AGENCIES, CASINOS, MOTOR VEHICLE DEALERS, NPOs, AUCTIONEERS, DEALERS IN PRECIOUS METALS ETC											
	Completed property sales (STRs)	Attempted property sales (SARs)	Casino (gambling related operations)	Vehicle Sales	NPOs (Churches etc)	Dealers in precious metals & stones	Auctioneering services	Accountant ants/Audito rs	Local authorities	Money Value Transfer Services (e-money etc)	Courier and Customs Clearing	Pension Fund
2018	1	0	0	2	0	0	0	0	0	0	0	1
2017	1	0	0	2	0	0	1	0	0	0	0	0
2016	0	0	3	5	0	3	3	0	0	7	0	1
2015	0	0	0	2	0	0	1	0	0	16	0	0

Table 10 STR reporting behaviour of the DNFBPs sector

	LEGAL PRACTITIONERS					
	Conveyancing (property sales)	Managing funds on behalf of clients in trust	STRs related to buying & selling of legal entities	Sourcing contibutions (capital) for the creation of legal persons / anything for creation of such persons	Management of legal persons, legal arrangements such as trusts etc	Fishing quotas
2018	0	0	0	0	1	0
2017	0	0	0	0	0	0
2016	2	1	0	0	0	0
2015	3	2	0	0	0	0

Table 11 STR reporting behaviour of the Legal Practitioners sectors

	ADLAs				
	Gift remittances	Maintenance remittances	Travelling remittances	Fake currency/note	Frequent sender/ Large amount
2018	1	0	0	3	21
2017	0	0	0	0	0
2016	6	1	1	0	23
2015	40	1	4	4	24

Table 12 STR reporting behaviour of the Lending Institutions sector

SECTION C: TERRORISM FINANCING (TF) RISK ASSESSMENT

7. TF threat and vulnerability assessment

The national TF threat in Namibia was assessed as **Medium** while the national TF vulnerability was assessed as **Medium High**, in the 2012 NRA. This resulted in the overall national TF risk being rated as **Medium High** using the above risk model. In 2014, an important milestone was attained when Namibia passed the Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014) (PACOTPAA). This laid the foundation on which a national TF combatting framework was created. This framework has largely informed the improvement in TF related control measures, thus reducing national TF vulnerability and enhancing the country's ability to mitigate TF threats.

7.1. TF threat assessment

In the 2012 NRA process, the National TF threat in Namibia was assessed as Medium with the National TF Vulnerability assessed as Medium High. This resulted in the overall National TF risk being rated as Medium High using the above risk model. The national threat level, in the current update is reduced to **Low-Medium**. The main factors underlying the TF Threat assessment in Namibia are:

a) The lack of confirmed cases of TF in Namibia;

b) Namibia and the whole of southern Africa being relatively peaceful and stable in comparison to other parts in the world (with the exception of terrorism related tensions being reported in Mozambique in recent years).

The assessment however took note of the global threat of terrorism and terrorist financing. This global threat escalates the potential for persons or institutions in Namibia to be involved in TF related activities directly or indirectly. The tables below show that there have been very minimal TF threats in Namibia over the last few years.

Year	2015	2016	2017	2018
Number of investigations conducted involving TF component	00	00	**01**	**01**
Number of TF prosecutions initiated	00	00	00	00
Number of convictions for TF	00	00	00	00
Details of the sanctions	00	00	00	00

Table 13 TF related investigations

Freezing, Seizure and Confiscation of TF related Assets Pursuant to UNSCR 1267	2015	2016	2017	2018
No. of cases involving freezing of TF related assets	00	00	00	00
Amount of TF related assets frozen	00	00	00	00
No. of cases involving seizure of TF related assets	00	00	00	00
Amount of TF related assets seized	00	00	00	00
No. of cases involving confiscation of TF related assets	00	00	00	00
Amount of TF related assets confiscated	00	00	00	00

Table 14 Freezing, seizure and confiscation of properties related to terrorism pursuant to UNSCR 1267

7.2. National TF vulnerability assessment

In assessing the national TF vulnerability in Namibia, the assessment considered the following key factors that impact National vulnerability in respect of TF:

a) The existence of a legal framework dealing with the combating of the financing of terrorism. At the time of conducting the 2012 NRA exercise, Namibia did not have a sound legal TF combatting framework in place. This has changed with the passing of the PACOTPAA. The Act significantly enhances the national combatting framework as combatting frameworks at institutional, regulatory/supervisory, LEA, prosecutorial and judicial levels are strengthened to deal with TF;

b) The 2012 NRA observed that there was incapacity to investigate and prosecute cases pertaining to TF. This position has since changed with the Ministry of Safety and Security having assumed the responsibility to coordinate all TF related combatting efforts as per the PACOTPAA;

c) The 2012 NRA also found that there were inadequate CFT preventative measures in respect of international funds transfers. This was due to the significant volumes and values of international trade, international funds transfers to and from “high risk” jurisdictions which were not monitored for potential suspicious transactions pertaining the financing of terrorism. With the PACOTPAA, such monitoring, albeit hindered by resource constraints in LEAs and the FIU, is taking place; and

d) The legal and institutional framework over Non-Profit Organizations (NPO's)[12] operating in Namibia: Before 2019, NPOs were not subjected to any TF supervisory monitoring and due diligence. The International AML/CFT/CPF standards (FAFT Recommendation 8) requires countries to have laws that effectively ensure NPOs are not abused to advance ML/TF/PF. In addition to the legal framework countries are required to ensure the following:

i) Effective supervision or monitoring of NPO's which are exposed to TF risks. Since late 2019, supervision and monitoring was entrusted to the FIC;

ii) All NPO's should be licensed or registered with information pertaining their purpose and objectives, identity of persons who own, control or direct their activities being publicly available. Although NPOs are licensed in terms of certain statues in Namibia, they were not subjected to the level of due diligence in line with the FATF Recommendations prior to 2019. Thus, control weaknesses still do exist at market entry level, despite measures now being undertaken to improve that;

iii) Appropriate measures in place to sanction violations of oversight measures. With NPOs being added to Schedule 1 of the FIA, it has become easier to administer compliance with oversight measures;

iv) Measures in place to provide access to beneficial ownership and control of trusts information available. This may be either publicly available such as through a national registry or only available to competent authorities. Despite there being room for improvement, there are some controls that assist in this regard, albeit to a limited extent as controls recently effected are still maturing;

v) Limited resources: TF investigation is a specialized field requiring certain expertise. LEAs generally agree that a lot need to be done to capacitate the relevant TF combatting task forces. Despite there being several capacity building activities including training and resourcing, there remains room for improvement; and

vi) The growing trend of financial instruments such as virtual currencies and money remittances, as well as the use of fictitious corporate structures, may also pose a

[12] See attached NPO Sectoral Risk Assessment Report on the NPO sector

certain level of risk. This was not sufficiently dealt with and will be explored in the 2020 NRA update.

Owing to the legal framework and other changes made after the passing of the PACOTPAA, Namibia capacitated her combatting framework to effectively participate in and meet her international obligations in the combatting of TF through her ability to perform extradition, mutual legal assistance, freezing, seizing of funds or property related to TF, prosecution or conviction of relevant persons. The national TF vulnerability level previously assessed as Medium High in 2012 is now revised to **Medium**.

SECTION D: SECTORAL VULNERABILITY ASSESSMENTS

8. Legal Practitioners Sector

8.1. Legal Practitioners Sector Overview

Legal Practitioners provide services that are generally vulnerable to potential ML abuse. It is for this reason that they are captured under the FIA as Accountable Institutions and need to have effective measures in place to mitigate ML/TF/PF risk exposure. The World Economic Forum identified the use of professional facilitators as one of two key enablers of money laundering, alongside the related activity of concealing beneficial ownership through complex corporate and trust structures for the purpose of illicit financial transactions.[13] This report presents a summary of the outcomes from the SVA, as well as methodology and techniques applied in obtaining same.

There are over 150 legal practitioners nationwide registered to avail different types of services. The services which are susceptible to ML activities include conveyancing transactions, the creation of legal persons, managing clients' funds etc. The sector comprises over 40 conveyancing legal practitioners, who are inherently availing a high-risk service.

As part of this exercise, the FIC observed that the conveyancing industry's annual revenues exceed NAD 262,050,808 as per data collected[14]. As per our estimation, and from part of the data collected, the few bigger law firms have an average size of 23,000 clients, whilst the smaller and medium sized firms have an average size of 1,000 clients.

Overall, the residual vulnerability rating for this sector is rated as **2.18 (medium)**, largely owing to the observed risk mitigating factors being partially effective at this stage.

8.2. Legal Practitioners Sector Vulnerability Factors

a) **Analysis by sales/product base:** The weighted vulnerability for this factor is 1.14. Although LPs facilitate high vulnerability transactions, 90% of the financing involved in such transactions emanates from financial institutions (e.g. banks). The annual value of sales for the period under review amounts to NAD 262,050,808 as per the data collected[15];

[13] World Economic Forum, Global Agenda Council on Organized Crime, Organized Crime Enablers, July 2012
[14] Stakeholders were requested to avail annual revenues ad this figure was obtained from such
[15] Stakeholders were requested to avail annual revenues ad this figure was obtained from such.

b) **Analysis by client geographic risk:** The weighted vulnerability rate for this factor is 2.09. This is attributed to the fact that LPs have a majority of Namibian clients;

c) **Analysis by the type of client/customer base:** A moderate rating of 3 was arrived at as most LPs have clients who are legal persons or persons in some other arrangements such as partnerships/trusts. The weighted vulnerability exposure for this category is 3.7, as most LPs have clients that are either legal persons or other type of arrangements;

d) **Role of Supervisory bodies and authority to enter the market:** This assessment has shown that fit and proper assessments are performed on legal practitioners before they are admitted into practice, in line with section 4(1)(a) of the Legal Practitioners Act 15 of 1995. FAP assessment are also done at point of application, and at point of being granted with a Fidelity Fund certificate. Secondly, the legal practitioners are required to be registered with the FIC before a fidelity fund certificate issued by the Law Society of Namibia. Further, If, during practicing a LP is detected of being dishonest during the fit and proper assessment stage, such a legal practitioner can be struck from the roll or prohibited from practicing in line with section 32 of the Act, should he or she no longer conform to any of the requirements of section 4 the Act.

   A rating of 5 was allocated to AIs with no supervisory bodies. This sector is supervised by the Law Society of Namibia as well as the FIC for AML/CFT/CPF purposes, and consequently this resulted in a low vulnerability weight of 2 (medium).

e) **Analysis by payment method:**

- Cash payments: It was observed that only 15% of the sector's client transactions were facilitated in cash;
- Electronic Funds Transfers (EFT): The sector indicated that on average 65 percent of their clients make use of EFT as a method of payment; and,
- Debit or Credit Cards: The amount of debit card payments as per the data collected in the sector is NAD 1,516,276.86[16] which is quite insignificant compared to the EFT's and cash payments transactions;

[16] LPs were requested to avail data related to debit card payments and this figure were obtained from such.

Accordingly, this sector has a vulnerability score of 2.43 (medium), primarily because EFTs are the most preferred method of payment, with cash as a method of payment being less preferred.

8.3. Vulnerability mitigating factors/controls

Some LPs do not have adequate controls in place to mitigate risks, or the controls are not implemented effectively or consistently. As per the analysis, the overall score of this sector is 1.19, indicating that the sector is partially compliant.

8.3.1. Vulnerability assessment results for individual AIs

The analysis on individual entities vulnerability to ML is summed up herein. The ratings of individual LPs within the sector ranges from low-medium to medium, i.e. lowest being 1.73 to 2.46 respectively. The analysis considered the different implementation and effectiveness levels of internal ML control frameworks in each individual institution.

Entity	Rating
LP 1	2.74
LP 2	2.46
LP 3	2.29
LP 4	2.29
LP 5	2.29
LP 6	2.28
LP 7	2.28
LP 8	2.28
LP 9	2.21
LP 10	2.20
LP 11	2.15
LP 12	2.15
LP 12	2.15
LP 14	2.14
LP 15	2.14
LP 16	2.14
LP 17	2.14
LP 18	2.03
LP 19	2.02
LP 20	2.00
LP 21	1.87
LP 22	1.73

Table:15 Vulnerability Assessment Results for individual LPs

8.3.2. Vulnerability assessment results per sector

In summary, the sector's overall vulnerability classification is medium, i.e. 2.18 as per the vulnerability calculation. Amongst others, this score is attributed to the inherent vulnerability exposure and the effectiveness of implemented controls. The scores of respective LPs within the sector ranges from low to medium, i.e., lowest being 1.58 and highest being 2.4 respectively. This is captured in the methodology employed (See the attached Annexure).

OVERALL VULNERABILITY CALCULATION- LENDING SECTOR		Vulnerability weight	Weighted score		
STRUCTURAL Vulnerabilities					40%
Supervisory Body	30%	2.75	0.83		
Authority to enter Industry	70%	2.75	1.93		
Total Structural Vulnerability	100%	5.50			
Average Structural Vulnerability		2.75	2.75		
Business (inherent) Vulnerability					60%
Total Sales/Product Base Vulnerability Exposure	10%	3.50	0.35		
Geographic Region Vulnerability	20%	1.00	0.20		
Customer Base Vulnerability	20%	2.00	0.40		
Delivery Channel Vulnerability	20%	1.00	0.20		
Lending Services	30%	2.5	0.75		
Total inherent vulnerability	100%	7.5			
Weighted average inherent vulnerability		1.88	1.90		
Vulnerability Mitigants					
Policies and procedures	25%	0.38	0.01		
Compliance Officer	5%	1.50	0.01		
Training	10%	0.19	0.00		
Reporting of STRs and CTRs	15%	0.56	0.01		
Aware of FIA obligations	15%	0.56	0.01		
In contact with FIC i.e. Training	5%	0.94	0.01		
Independent check- internal and external audit	10%	0.38	0.01		
Total Vulnerability Mitigants	85%	4.50			
Average Vulnerability Mitigants		0.64	0.06		
Overall Residual Vulnerability Score		2.18			

Table 16: Overall ML vulnerability calculation: Lending Sector

8.4. 2019 Update

In keeping with emerging trends and risks, the FIC has learned about emerging risks and vulnerability during the last quarter of 2019, related to the famous Fishrot scandal pertaining this sector. Upon suspicious transactions and activities received from the regulated populace as well as the current on-going court case challenge, as well as media broadcasts, the FIC Compliance and Monitoring Division conducted targeted FIA Compliance Assessments. The aim and scope of the assessments were mainly to assess the controls that were comprised by the various legal practitioners who facilitated

transactions for individuals and companies that were involved in the Fishrot scandal. As such, the assessment was done by analysing specific transactions as conducted by those individuals, as well as by assessing the CDD and EDD conducted on those individuals. The vulnerabilities observed are outlined below.

8.4.1. ML/TF Risks/vulnerabilities observed during the assessments

a) Inadequate CDD and EDD controls applied

The assessment found that overall, observed inadequacies in the conducting of EDD, especially relating to client's financial profiles on sources of income and funds across the law firms that were assessed. The assessment in general found that non-compliance with sections 23 and 24 of the FIA, coupled with section 25 of the Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014) (PACOTPAA). The inadequacies points to the nature and purpose of transactions of the transactions conducted, as well as the screening of clients against the UNSC sanction lists that were mostly not documented and or available in the files assessed.

This was observed particularly with transactions involving high financial values, or those that are conducted by high risk clients. If the source of funds used in transactions is not in line with the known client financial profile or source of income/occupation, such transaction could expose the services of law firms, and the overall sector to potential ML abuse. Equally, the purpose and nature of transactions may not have been duly considered in certain transactions, as far as the disbursing of finances from certain sources was concerned.

Noteworthy to mention, although most of the transactions assessed dated back past 2018, and improvements are noted in the identified shortcomings of the sector to date, past 2018.

b) Abuse of trust accounts

In terms of the Legal Practioners Act,[17] lawyers who holds fidelity fund certificates for the purposes of managing trust accounts, to keep proper books of account of client monies. The aim of the trust account is for the legal practitioner to exercise exclusive control as trustee, agent or stakeholder or in any other fiduciary capacity over the trust monies. This assessment observed that the modus

[17] Section 25 & 26 of Act 15 of 1995, read Rules 17 & 18 of the Rules of the Law Society.

operandi involved in some of the law firms operations was that funds would be deposited to lawyer's trust accounts for supposed legal services paid.

In contrast, upon a closer scrutiny, by following the trial of the disbursements of the transactions of the trust, transfers were made out of the lawyers accounts to the various individuals bank accounts from the initial amount deposited. This is reflective of a typical transactional pattern of an account at a commercial banking institution and not that of a trust account of a lawyer, which is supposedly only for the receipt of a monies for legal services rendered, or for the managing of client monies such as bail monies, or those monies over which the legal practitioner exercises exclusive control as trustee, agent or stakeholder or in any other fiduciary capacity. Shortcomings related to this were also CDD and EDD controls, (sections 21,22 and 23 of the Act) that were observed due to the fact that inadequacies related to the nature and purpose of transactions conducted, were mostly not documented and or available in the files assessed. Hence there was no correlation to the purpose of the transactions compared to the nature of services that the law firm offers.

c) The manipulation of property values

The FIC observed that adequate due diligence was not conducted in determining and concluding on properties values acquired through conveyancing services. For example, a property was acquired for a value that was less than its usual valuation. The known trend is that criminals may be drawn to money laundering through real estate due to the fact that it is relatively uncomplicated and requires little expertise. This happens mainly due to the inability to detect over or under valuations. Criminals may overvalue real estate with the aim of obtaining the largest possible loan from a lender. The larger the loan, the greater the amount of illicit funds that can be laundered to service the debt. Alternatively, under-valuation involves recording the property value on a contract of sale which is less than the actual purchase price.

The difference between the contract price of the property and its true worth is paid secretly by the purchaser to the vendor using illicit funds. The criminal (purchaser) is able to claim that the amount disclosed in the contract as having been paid is within their legitimate financial means. If the property were sold at the market or higher value, the apparent profits would serve to legitimize the illicit funds. In other words, Illicit actors often omit a part of the price from the purchase contract. In other words,

according to FATF[18] the amount listed on the contract of sale is less than the real purchase price paid. The price shown on the contract is paid for with a mortgage loan; whereas the part not appearing on the contract is paid in cash produced by the criminal organisation or terrorist group's criminal activities and is paid to the seller under the table.

d) Inadequate transaction monitoring and ability to detect unusual and suspicious transactions

The FIC also observed with concern that, as a result of the inadequacies and shortcomings in the above findings, (8.4.1 a – d) the law firms were unable to monitor and detect transactions as expected in line with sections 23 and 24 of the FIA. This is largely owing to the absence of crucial client financial profile information (source of income/funds) and information on the nature and purpose of the transaction, as stated in findings above.

The shortcomings identified will be dealt with as part of the action plan going forward in the alignment of our supervisory and monitoring activities as documented below.

9. Lending Sector

9.1. Lending Sector Overview

Personal and business lending, including property or asset finance lending are not often perceived as services highly vulnerable to ML threats. Lending Institutions are registered and licensed by various bodies depending on a form of such institutions. Some institutions are established by acts of parliament and these enabling acts indicate how such entities should be registered. Fit and Probity assessments are performed at the licensing and establishment of lending institutions as per FATF Recommendations to reduce the risk of licensing beneficial owners or management who may expose lending services to potential ML risks.

The Lending sector herein includes institutions such as the Development Bank of Namibia, National Housing Enterprises, Agricultural Bank of Namibia, Environmental Investment Fund and First Capital Housing Fund. This excludes mortgage financing offered by banking institutions as such are covered

[18] FATF Typology Paper: Money Laundering & Terrorist Financing Through The Real Estate Sector. Available at: https://eurasiangroup.org/files/FATF_docs/ML_and_TF_through_the_Real_Estate_Sector.pdf

under the SVA of the banking sector. Micro lenders under the supervision of the Namibia Financial Institutions Supervisory Authority (NAMFISA) are also not included in this sector. NAMFISA has already undertaken similar studies for sectors under its supervision.

Lending Institutions are generally used to launder funds in several ways including the use of proceeds from illicit activities to repay loans. The common trend is seen through early repayment or settlement of loans through the use of funds derived from illicit activities. Often, the opportunity for ML in this area occurs where loan repayments are made in cash (or transferred to lender) and the source of funds for large payments (usually in cash) is unclear. Equally, proceeds (funds) from illicit activities can be used to acquire assets and such assets can be used as security to source loans. Accountable Institutions issuing such loans naturally find this method of laundering much more challenging to detect as the financial history of acquiring such assets is not always known.

The type of Lenders in this sector include those involved in the agricultural, mortgage[19], small and medium enterprises and environmental industries.

Overall, the analysis found that the ML vulnerability level in the sector is medium. The major factors that contribute to vulnerability include the noted ineffective AML controls at institutional level and the significantly higher transactional values traded in. On the other hand, the due diligence carried out, primarily for Lenders to establish client's ability to repay loans (credit worthiness) entail measures that ascertain client's financial profiles, sources of funds/income etc. The credit management exercise, to a certain extent inherently minimizes the risk of lenders availing services to persons who cannot demonstrate legitimate sources of income or funds. What is vital is for the sector to understand that most CDD information sourced for credit worthiness assessments can be equally used for AML purposes.

The sector has 5 key role players, offering the above mentioned products and services. The entities are Agricultural Bank of Namibia, the Environmental Investment Fund, First Capital Fund, National Housing Enterprises (NHE) and the Development Bank of Namibia. As per data collected from the sector and annual reports, the average asset size of the above mentioned firms for the period under review is NAD 1,769,158,301.50. The annual average value of sales for the period under assessment

[19] Only the National Housing Enterprises (NHE), which offers mortgage house financing to low and medium income clients is included in the Lending sector.

amounts to NAD 4,254,548,426 as per the data collected[20]. The average AI has a client base ranging from 1,000-1,200, with the exception of the Environmental Investment Fund that has less than 10 clients, and the Agricultural Bank that has about 6,200 clients. The vulnerability rating for this sector for the period under review is at **2.18 (medium)**.

9.2. Vulnerability Factors

In this sector, indicators of inherently higher vulnerability are loans settled in shorter periods, loans by certain types of customers as well as the quality and implementation of ML vulnerability management controls. The next sub-section explains how the analysis arrived at vulnerability ratings.

a) **Analysis by sales/product base:** The weighted vulnerability for this factor is 3.50, which falls within the medium-to-high vulnerability level. This is mainly attributed to the high values and volumes in total sales across the entire sector.

b) **Analysis by client geographic risk:** The weighted vulnerability exposure for this sector, in terms of this evaluation category is 2.00 (medium). It appears the majority of Lenders (75%) of the sector have legal persons as clients with insignificant foreign beneficial owners/clients.

The overall weighted vulnerability rate in terms of this factor is 1.00 (low). This is mainly attributed to the fact that all the Lenders have granted loans to only Namibians in the reviewed period.

c) **Analysis by the type of client/customer base:** The FIA compliance assessment activities conducted in the sector indicate that in most cases, beneficial owners' information was not obtained when business relationships were established in the sector. A moderate rating of 3 is allocated to Lenders with clients who are legal persons.

e) **Supervisory bodies and authority to enter market:** The key players in the lending space are mostly government owned financial institutions such as the Development Bank of Namibia, Agricultural Bank of Namibia, the National Housing Enterprises, and the Environmental Investment Fund (EIF). The shareholder is the state and these entities are established through acts of parliament. Directors are usually appointed in terms of the specific acts of parliament which creates the entities. Thus far, there is no indication that the fit and probity evaluations are

[20] This figure excludes annual sales revenue for one lending sector that failed to provide same to the FIC.

compliant with AML/CFT expectations. All indications suggest that competence (experience and qualifications) is the criteria for appointing directors.

Since this sector is regulated by the FIC for ML/TF/PF purposes. The vulnerability weight for this category is 2.75 (medium).

f) Analysis by payment method

a) Cash payments: It was observed that only 3% of clients repay loans in cash compared to other forms of payment;

b) Electronic Funds Transfers (EFTs): The survey results indicate that 95 percent of lenders' clients made use of EFT payments;

c) Debit or credit Cards: Overall, it was observed that users do not make use of debit/credit cards when repaying loans;

d) Lending services: The analysis of this section of the data took into account the dynamics above and it was observed that an average of 30 percent (NAD 1 276 364 528) of loans are settled earlier. Accordingly, the vulnerability weight for this category is 2.50 (medium).

9.3. Vulnerability mitigating factors/controls

As per the analysis, the overall score of this sector in terms of AML control implementation is 0.64, indicating that the sector is partially compliant. Some Lenders do not have adequate controls in place to mitigate vulnerabilities, or the controls are not implemented effectively or consistently.

9.4. Vulnerability assessment results for individual AIs

The ratings of individual Lenders within the sector ranges from low-medium to medium, i.e., lowest being 1.65 and highest being 2.85 respectively. The analysis considered the different implementation and effectiveness levels of internal ML control frameworks in each individual institution, as per below table

Institution	Rating	Vulnerability Score
Lender A	2.85	Medium
Lender B	2.22	Medium
Lender C	1.98	Low-medium
Lender D	1.65	Low-medium

Table 17: Individual Vulnerability Ratings

As seen above, Lender D has the lowest ML vulnerabilities since most mitigating controls are in place, followed by Lender C.

9.5. Vulnerability assessment results per sector

In summary, the sector's overall vulnerability classification is 'medium'. It was calculated at an average of 2.18, as per the methodology employed.

Amongst others, this score is attributed to the inherent vulnerability level as observed in the sector. The FIC also considered the mitigating controls prevalent in the sector in terms of their contribution to the residual level of vulnerability. Equally, the individual Lending scores, as summed up above, within the sector aggregated the final score.

OVERALL VULNERABILITY CALCULATION- LENDING SECTOR		Vulnerability weight	Weighted score		
STRUCTURAL Vulnerabilities					***40%***
Supervisory Body	30%	2.75	**0.83**		
Authority to enter Industry	70%	2.75	**1.93**		
Total Structural Vulnerability	100%	**5.50**			
Average Structural Vulnerability		**2.75**	**2.75**		
Business (inherent) Vulnerability					***60%***
Total Sales/Product Base Vulnerability Exposure	10%	3.50	**0.35**		
Geographic Region Vulnerability	20%	1.00	**0.20**		
Customer Base Vulnerability	20%	2.00	**0.40**		
Delivery Channel Vulnerability	20%	1.00	**0.20**		
Lending Services	30%	2.5	**0.75**		
Total inherent vulnerability	100%	**7.5**			
Weighted average inherent vulnerability		**1.88**	**1.90**		
Vulnerability Mitigants					
Policies and procedures	25%	0.38	**0.01**		
Compliance Officer	5%	1.50	**0.01**		
Training	10%	0.19	**0.00**		
Reporting of STRs and CTRs	15%	0.56	**0.01**		
Aware of FIA obligations	15%	0.56	**0.01**		
In contact with FIC i.e. Training	5%	0.94	**0.01**		
Independent check- internal and external audit	10%	0.38	**0.01**		
Total Vulnerability Mitigants	85%	**4.50**			
Average Vulnerability Mitigants		**0.64**	0.06		
Overall Residual Vulnerability Score		2.18			

Table 17: Overall vulnerability assessment results for the Lending sector

10. Customs Clearing and Forwarding Agents (CCFAs) Sector

10.1. Sector ML/TF/PF Sector Overview

As at 01June 2020, the total number of CCFAs registered with the Ministry of Finance amounted to 314. They are licensed under three (3) categories, namely:

No:	Customs Clearing Agents	Purpose
1	999	For Customs Purposes. Only make use by Namibia Customs and Excise Personnel
236	6 x alpha - numeric	Clearing Agents, who can do clearance for anyone for a fee
77	10 x alpha - numeric	Direct Trade Inputs meant only to do their own clearance
314		

Customs Clearing and Forwarding Agent's services are inherently vulnerable or susceptible to potential ML abuse due to the following factors:

i. the industry does not have an active regulatory body to monitor their activities; Compliance behaviour is thus not enforced to a level that encourages AML efforts;
ii. the industry is exposed to a variety of clients that may possess or potentially launder proceeds from illicit activities;
iii. Some agents are given responsibilities of making payments on behalf of their clients and have therefore exposed the industry to launder money knowingly or unknowingly.

Namibia is a member of the Southern Africa Customs Union (SACU). Customs regulations are documented in the Customs and Excise Act (Act no. 20 of 1998) and conform to most international conventions relating to recommended practices regarding the import and export of goods. Although CCFA are being licensed in terms of section 73 of Customs and Excise Act, it is worth noting that the FIC does not have reasonable assurance that the existing licensing measures meet the fitness and propriety expectations recommended by the FATF[21] to reduce the risk of licensing beneficial owners

[21] The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

who may expose CCFA' services to potential ML risks. When such licensing measures were implemented, the FIA was not yet in place.

Overall, the sectorial vulnerability rating of this sector is rated as **medium high (3.88)**, primarily owing to ineffective licensing and regulatory shortcomings and the absence of vulnerability mitigating factors within the sector.

10.2. Risk Factors

The vulnerability factors considered were a combination of the analysis relating to the following:

a) **Sales/product base:** According to our review of the Customs Clearing and Forwarding Agent's incoming bank transactions, Total sales turnover for the top Eighty (80) CCFA for the period was NAD 61 billion for the 2017 and 2018 period. Accordingly, The Namibian Statistics Agency indicated that , the country's total value of imports to Namibia was recorded at NAD 89, 043 Billion and NAD 110, 219 Billion for the 2017 and 2019, respectively (Namibia Statistics Agency, 2018).

   Overall, the exercise assessed the sector's vulnerabilities at a weighted rating of 1.10. This low vulnerability rating was as a result of low volumes of sales including other secure payment options i.e. EFTs, SWIFT and cards.

b) **Geographic risk:** Agents with clients from international jurisdictions and jurisdictions that are high risk, based on reported incidents and jurisdictions listed by the FATF as high risk are more exposed to vulnerabilities [22]. According to this study, it was also noted that some CCFA receive or remit funds to some jurisdictions listed by the FATF as non-cooperating countries including other jurisdictions identified as high risk for capital flight and tax evasion in Namibia. China has also been added to this list by the FIC because it was found to expose Namibia to ML and TF risks as uncovered during the 2014 National Risk Assessment exercise. The total

[22] High-risk and other monitored jurisdictions:
The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in two FATF public documents that are issued three times a year. The FATF's process to publicly list countries with weak AML/CFT regimes has proved effective (click here for more information about this process). As of October 2018, the FATF has reviewed over 80 countries and publicly identified 68 of them. Of these 68, 55 have since made the necessary reforms to address their AML/CFT weaknesses and have been removed from the process (see also, an overview of the jurisdictions currently identified in this process).

amount of money in NAD remitted by Namibians to these Jurisdictions including China for the 2018 and 2018 financial years are as follows:

Outflow to Country	2017	2018
The Bahamas	28,864,317.04	71,148,414.17
Botswana	3,153,064,694.54	2,575,271,267.29
Cambodia	.00	47,903.57
Ethopia	1,722,672.01	5,101,556.36
Ghana	4,537,168.62	4,214,923.02
Pakistan	956,528.66	2,542,051.77
Panama	1,315,565,861.35	155,691,374.33
Sri Lanka	455,472.12	298,931.29
Syria	.00	.00
Trinidad and Tobago	25,323.08	.00
Tunisia	5,440,725.65	5,323,686.48
Yemen	6,335.05	.00
China	695,004,159.36	2,162,401,195.59

Table 18: High-risk and other monitored jurisdictions 2017 and 2018 Outflow

A rating of 4.93 was recorded for the sector due to the high percentage of foreign client's base within the CCFA sector.

c) International Inflow received: The total amount of international funds inflows for the 2017-2018 financial period was estimated to be NAD 166,567,696,481.75. Nonetheless, Total international inflow received by our top 80 CCFA is 20,675,993,294.86.

d) International outflow remitted: The total amount of international funds outflow for the 2017-2018 financial period is NAD 101,941,104,141.29. Total international outflow remitted by our top 80 CCFA is NAD 5,914,830,242.84. The top 10 countries in this regard are: South Africa, United States, Germany, Switzerland, Botswana, United Kingdom, China, Luxemburg, Belgium and France.

e) Type of client/customer base: The customs Clearing and forwarding services are equally consumed by both natural persons and legal persons.

f) **Supervisory Bodies and Market entry:** CCFA are licensed and regulated by the Ministry of Finance as per the Customs and Excise Act (Act no. 20 of 1998). However, the sector did not have an AML supervisory body previously as it was not identified amongst sectors exposed to ML, TF and PF risks. Recent developments and recent typologies have rendered the CCFA exposed to ML/TF/PF risks.

AIs or RIs in sectors that have AML and licensing supervisory bodies are perceived to present lower ML risks. The CCFA sector was recently only included as an Accountable Institution in terms of Schedule 1 of the FIA and has therefore it has not yet been assessed for ML/TF/PF risk exposure. Various short comings were noted as far as ML/TF/PF risks are concerned. According to this study, the agents are not required to submit a police clearance certificate and there is no fixed system in place to identify and obtain the ultimate beneficial ownership information. However, the requirements make provision for Suspension and Cancellation procedures applied when licensed CCFAs breach their licensing requirements. This subsequently resulted in a higher risk weighting of 4.

g) **Methods of payment:** Below is a summary of the sector's responses:

i. **Cash payment:** On average, 19% of clients use this method of payment;

ii. **Electronic Fund Transfers (EFTs):** 55% of industry payments are made via EFT

iii. **Debit Cards and Credit Cards:** This form of payment allows the holder to transfer money electronically from their bank account when making a purchase. The risk exposure through this form of payment is perceived to be moderate since these funds are within a financial institution which is perceived to have AML controls in place. The expectation, if controls are effective, is that such account from where the funds emanate was subjected to the necessary customer due diligence and relevant risks mitigated. The credit card allows the holder to purchase goods or services using credit extended by financial institutions. The risk exposure from this form of payment is perceived to be moderate since such funds are with a financial institution which is perceived to have controls in place. Only 1% of payments within the sector are made using cards.

iv. **SWIFT Bank Payments:** About 25% of payments made and received within the Sector are payments meant for other jurisdictions which are processed via the SWIFT system.

v. **Payments on behalf of 3rd parties:** 48% of the agents indicated that they make payments on behalf of their clients to suppliers etc.

10.3. Vulnerability Mitigating Factors/ Controls

As stated above, in order to arrive at the residual risk rating, the assessment took into consideration implementation of controls as required by the FIA and the extent of such controls being effectively implemented.

The Ministry of Finance mostly recently (September 2019) included CCFAs to schedule 1 of the FIA as Accountable Institutions. There was previously no legal obligation for the sector to implement AML/CFT controls. Hence, the sector has not implemented any AML/CFT controls, and therefore are perceived to have a high ML risk exposure.

However, a few CCFAs have indicated to have controls in place to safeguard their businesses from trade-based ML, tax evasion and capital flight risk exposures.

This was the first CCFAs industry assessment aimed at understanding the ML and TF risk exposure and other behavioral patterns within the sector. In the meantime, the FIC has also begun sectoral engagements, conducted training and awareness sessions despite low attendance in an attempt to assist the sector with the Implementation of FIA control measures.

As a result of this study, the FIC has put in place a 3-year strategic plan that will ensure that all CCFAs are registered, different monitoring and supervisory activities are conducted effectively, and the sector is accorded the support and training it needs to resolve challenges they may face.

A reduced rating was affected to the CCFAs who were found to have implemented controls that could/may potentially reduce their ML/TF risks exposures.

10.4. Case studies observed in Namibia

The case studies showing how threats undermined controls within the CCFAs and importing sector are captured under section 6.2.1(a)(ii) of this report.

Financial Sector concerns/control weaknesses exploited in above case studies:

a. Insufficient understanding of customs processes;
b. Lack of avenues for verifying authenticity of customs documents presented by importers: To date, Namibia does not have a system which enables the comparison of records declared at customs with actual remittances made at financial institutions;
c. Lack of avenues to ensure customs documents used to remit through one bank are not reused at other banks;
d. EXCON Rulings: Over reliance on importers/clients. With advance payments, importers may make payments using only pro-form invoices. The expectation is that such importers will, within 6 months from the time of having made such remittances, avail the banks with complete set of import documents (e.g. SAD500 along with invoices, release orders/exit notes, bills of ladings etc.).

10.5. Vulnerability assessment results per sector and per AI

The CCFA sector's overall vulnerability classification is deemed **medium high at 3.88** out of **5** as per the vulnerability calculation (*Refer to table below*). This score is partly attributed to the inherent vulnerability observed in the sector.

OVERALL VULNERABILITY CALCULATION - Customs Clearing and Forwarding Agents		Vulnerability weight	Weighted score	
STRUCTURAL VULNERABILITY				*40%*
Supervisory Body	30%	4.00	**1.20**	
Authority to enter Industry	70%	4.00	**2.80**	
Total Structural Vulnerability	100%	**8.00**		
Average Structural Vulnerability		**4.00**	**4.00**	
Business (inherent) vulnerability				*60%*
Total Sales/Product Base vulnerability Exposure	20%	1.10	**0.22**	
Geographic Region vulnerability	20%	4.93	**0.99**	
Customer Base vulnerability	30%	4.50	**1.35**	
Delivery Channel vulnerability	30%	1.81	**0.54**	
Total inherent vulnerability	100%	**12.3**		
Weighted average inherent vulnerability		**3.08**	**3.10**	
The Bahamas		0.00		
Botswana		3.00		
Cambodia		0.00		
Ethopia		0.00		
Ghana		0.00		
Pakistan		0.00		
Panama		0.00		
Sri Lanka		0.00		
Syria		0.00		
Trinidad and Tobago		0.00		
Tunisia		0.00		
Yemen		0.00		
China		2.00		
Others		14.00		
Overall Residual Vulnerability		**3.88**		

Table 19: Overall Vulnerability Calculation for the sector

Secondly, the absence of mitigating controls in the sector contributed to the residual vulnerability. At individual entity level, the assessed Agents scores within the sector where also considered to arrive at the final vulnerability. Vulnerability rating of Agents in this category ranges from medium to high, i.e., with the lowest being 3.4 and highest being 4.08 respectively.

No	Entity	Rating		No	Entity	Rating
1	AI 1	4.08		42	AI 42	3.96
2	AI 2	4.01		43	AI 43	3.96
3	AI 3	3.98		44	AI 44	3.96
4	AI 4	3.97		45	AI 45	3.96
5	AI 5	3.96		46	AI 46	3.96
6	AI 6	3.96		47	AI 47	3.96
7	AI 7	3.96		48	AI 48	3.96
8	AI 8	3.96		49	AI 49	3.96
9	AI 9	3.96		50	AI 50	3.96
10	AI 10	3.96		51	AI 51	3.96
11	AI 11	3.96		52	AI 52	3.96
12	AI 12	3.96		53	AI 53	3.96
13	AI 13	3.96		54	AI 54	3.96
14	AI 14	3.96		55	AI 55	3.96
15	AI 15	3.96		56	AI 56	3.96
16	AI 16	3.96		57	AI 57	3.96
17	AI 17	3.96		58	AI 58	3.96
18	AI 18	3.96		59	AI 59	3.96
19	AI 19	3.96		60	AI 60	3.96
20	AI 20	3.96		61	AI 61	3.96
21	AI 21	3.96		62	AI 62	3.96
22	AI 22	3.96		63	AI 63	3.96
23	AI 23	3.96		64	AI 64	3.96
24	AI 24	3.96		65	AI 65	3.96
25	AI 25	3.96		66	AI 66	3.96
26	AI 26	3.96		67	AI 67	3.96
27	AI 27	3.96		68	AI 68	3.60
28	AI 28	3.96		69	AI 69	3.54
29	AI 29	3.96		70	AI 70	3.52
30	AI 30	3.96		71	AI 71	3.50
31	AI 31	3.96		72	AI 72	3.48
32	AI 32	3.96		73	AI 73	3.47
33	AI 33	3.96		74	AI 74	3.46
34	AI 34	3.96		75	AI 75	3.43
35	AI 35	3.96		76	AI 76	3.43
36	AI 36	3.96		77	AI 77	3.41
37	AI 37	3.96		78	AI 78	3.40
38	AI 38	3.96		79	AI 79	3.37
39	AI 39	3.96		80	AI 80	3.35
40	AI 40	3.96			**Sector Average**	3.88
41	AI 41	3.96				

Table 20: Individual Vulnerability Calculation per CCFA.

10.6. Challenges Observed

The *modus of operandi* was that the FIC obtains bank statements of all CCFAs from all local banks and analyze such bank statements. A Vulnerability Assessment questionnaire was completed by all CCFAs and processed via the Vulnerability Assessment Tool. The results of the Vulnerability Assessment tool based on the questionnaire responses and the information relating to the CCFAs from Bank of Namibia's Exchange Control Department and activities as per the bank statements were used to rank the sector.

Some challenges specific to this sector includes:

At the time of the assessment, the sector was not captured by the FIA and most agents were not yet registered with the FIC. As a result, some CCFAs could not be reached on time or at all, this rendered the process ineffective and delayed completion of certain phases of the project. The FIC had to obtain address details and directly engage stakeholders.

i. Despite various efforts, only a few CCFAs turned up for the 2 meetings that were scheduled. In total the FIC collected 21 completed questionnaires.

ii. The meeting and input sought was only conducted in the coastal part of Namibia. Other meetings are scheduled to take place at various points of entry into Namibia (borders) in 2020. Therefore, results / information as highlighted in this report reflect the answers provided by the coastal agents. It is also worth noting that of the 314 CCFAs registered with the Ministry, 121 (39%) operated from the coastal border post of Walvis Bay during the 2018/2019 calendar years

11. Auctioneering Sector

11.1. Auctioneering sector Overview

The FIC has a record of twenty-one Auctioneers that are registered for FIA compliance supervision and monitoring purposes. Like other sectors, the Auctioneer sector is susceptible to ML/TF/PF threats. Auctioneering services provide an easier platform through which funds could be laundered or integrated in the financial system with minimum due diligence. This makes the sectors inherently vulnerable to ML activities. Some typical examples of how criminals can take advantage of Auctioneering services include:

i. taking advantage of a highly cash intensive environment to exchange ill-gotten proceeds/money for high value items; and
ii. criminals requesting unsuspecting Auctioneers to facilitate the auctioning or disposal of their high value items (acquired with proceeds of crime or from crime). Once a transaction is completed, proceeds of such a transaction are transferred via Electronic Fund Transfers or other means to the criminal's bank accounts and presented as legitimate earnings.

Overall, a sectoral residual vulnerability rating of **medium high (3.45)** was recorded for the sector. This is a medium-high rating predominantly owing to the vulnerability mitigating factors being partially effective.

11.2. Vulnerability Factors

Indicators of higher vulnerability within the Auctioneer Sector includes large volumes of cash transactions, the absence of a prudential supervisory body as well as the quality and implementation of AML/CFT/CPF controls.

a) **Analysis by Sales/product base:** The overall risk weight was recorded at 1.5. This Low-Medium vulnerability rating was attributed to the Auctioneers' overall sales revenue being insignificant when compared to other sectors, nationally. Within the sector, this study also found that the percentage of sales paid in cash is low, which is about 21% of total sales for the period under review.

b) Analysis by client geographic risk: Auctioneers with clients from high risk Jurisdictions, based on reported incidents and jurisdictions listed by the FATF and the United Nations Security Council (UNSC) as high risk present a higher risk of exploiting the vulnerability of services in the sector. Generally, Auctioneers' weighted vulnerability rating in terms of this factor was recorded as 2. The low–medium rating was attributed to a fair presence of foreign clients amongst the Auctioneers' clientele. The percentage of foreign clients in the sector for the period under review averaged 14.20%.

c) **Analysis by the type of client/customer base:** A medium to high weighted vulnerability rating of 3.20 is allocated to the Auctioneers sector. The majority of Auctioneers were observed to have a combination of legal and natural persons and a foreign client base.

d) **Analysis based on the presence/role of Supervisory Bodies and Authority to enter Market:** The sector does not have a direct prudential supervisory body that is responsible for the fit and proper assessments on beneficial owners or individuals that hold management positions. This may also be brought about by the presence of different types of auctioneers in the sector, namely those specializing in the auctioneering of motor vehicles, property, livestock and loose goods.

The ministry of Agriculture: Veterinary services and Livestock Agents Brokers and Transporters Association (LABTA) is responsible for the registration of livestock, while the Namibia Estate Agent's Board (NEAB) is responsible for the registration of Estate Agents. The respective auctioneers therefore register with the regulatory bodies of the services that they provide. The other bodies such as Business and Intellectual Property Authority (BIPA) are for administration and

licensing purposes only, hence the need for a stricter central body responsible for the registration of all auctioneers.

It is the FIC's view that the absence of a sectoral supervisory body to enforce prudential requirements presents greater vulnerabilities to the Auctioneering sector. Due to reasons given above, the Auctioneers weighted risk rating in this category was calculated at 5. Auctioneers are regulated for ML/TF/PF activities by the FIC.

e) **Analysis by payment method:** For the sector, 22.33% of sales in the year under review were financed through cash. The Auctioneers sector scored a weighted vulnerability rate of 2.89 in this category. This indicates that Auctioneers are more cash intensive institutions compared to other sectors such as legal practitioners, motor vehicle dealers etc., that facilitate transactions which are normally bank financed.

11.3. Vulnerability Mitigating Factors/ Controls

The overall score of this sector in terms of control implementation is 0.52. This rating indicates that the sector has minimum controls in place and/or the ineffective implementation thereof. The sector therefore remains exposed to the highest level of vulnerability.

11.3.1. Vulnerability assessment results for individual auctioneers

The rating scores of individual auctioneers ranged from "medium" to "medium-high". The auctioneer with the lowest score was rated 3.00 and the highest was rated 3.67 respectively. The analysis considered the different implementation and effectiveness levels of internal ML control frameworks in each individual institution.

Entity name	Rating
Auctioneer 1	3.67
Auctioneer 2	3.64
Auctioneer 3	3.59
Auctioneer 4	3.57
Auctioneer 5	3.56
Auctioneer 6	3.47
Auctioneer 7	3.47

Auctioneer 8	3.47
Auctioneer 9	3.47
Auctioneer 10	3.47
Auctioneer 11	3.47
Auctioneer 12	3.47
Auctioneer 13	3.47
Auctioneer 14	3.47
Auctioneer 15	3.47
Auctioneer 16	3.47
Auctioneer 17	3.47
Auctioneer 18	3.37
Auctioneer 19	3.33
Auctioneer 20	3.00

Table 21: Vulnerability Assessment results per individual Auctioneer

11.4. Vulnerability assessment results per sector

OVERALL VULNERABILITY CALCULATION - AUCTIONEER SECTOR		Vulnerability weight	Weighted score	
STRUCTURAL VULNERABILITY				*40%*
Supervisory Body	30%	5.00	**1.50**	
Authority to enter Industry	70%	5.00	**3.50**	
Total Structural Vulnerability	100%	**10.00**		
Average Structural Vulnerability		**5.00**	**5.00**	
Business (Inherent) Vulnerability				*60%*
Total Sales/Product Base Vulnerability Exposure	20%	1.50	**0.3**	
Geographic Region Vulnerability	20%	2.00	**0.40**	
Customer Base Vulnerability	30%	3.20	**0.96**	
Delivery Channel Vulnerability	30%	2.89	**0.87**	
Total inherent Vulnerability	100%	**9.6**		
Weighted average inherent Vulnerability		**2.40**	**2.53**	
Vulnerability Mitigants				
Policies and procedures	25%	0.40	**0.01**	
Compliance Officer	10%	1.85	**0.03**	
Training	15%	0.18	**0.00**	
Reporting of STRs and CTRs	15%	0.10	**0.00**	
Aware of FIA obligations	15%	0.70	**0.02**	
In conduct with FIC i.e. Training	10%	0.33	**0.00**	
Independent check- internal and external audit	10%	0.10	**0.00**	
Total Vulnerability Mitigants	100%	**3.65**		
Average Vulnerability Mitigants		**0.52**	0.07	
Overall Residual Vulnerability		**3.45**		

Table 22: Vulnerability assessment results for the Auctioneer sector

The sector's final vulnerability classification is "Medium-High. It was calculated at an average of 3.45 as per the methodology employed. This score is attributed to the inherent vulnerability observed in the sector, amongst others, the ease of market entry, a moderate cash intensive environment, and the absence of effective functioning AML/CFT/CPF control measures. Additionally, the absence of market entry controls for auctioneers specializing in motor vehicles, goods and livestock auctions also enhances AML and CPF risks as the licensing authorities and do not provide any supervisory activities which can aid FIA compliance.

The ineffective mitigating controls in the sector ultimately aggravated the residual vulnerability. Controls relating to inadequate implementation of policies and procedures, non-reporting of STRs and CTRs and the absence of independent audit reviews on FIA controls[23] greatly impacted the rating.

12. Casino Sector

12.1. Casino Sector Overview

Casino services are inherently vulnerable or susceptible to potential ML abuse due to the following factors:

i. the industry does not have an active prudential regulatory body to monitor their activities, Compliance behaviour is thus not enforced to a level that encourages AML efforts;
ii. the industry is exposed to a variety of clients that may possess or potentially launder proceeds from illicit activities;
iii. Casinos are cash intensive businesses with relatively reduced customer due diligence controls; and
iv. Casinos offer various financial services (e.g. foreign exchange and cash ins and cash outs) [24].

Casinos are licensed by the Gaming Control Division, which is governed by the Casinos and Gambling Houses Act, (Act 32 of 1994). The existing licensing measures do not meet the fitness and propriety expectations of Recommendation 26 by the FATF[25] to reduce the risk of licensing beneficial owners

[23] observed with the majority of auctioneers across the sector
[24] FATF Vulnerabilities of Casinos and Gaming sector report (March 2009)

[25] The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

who may expose Casino services to potential ML risks. However, the sector has, to a certain degree, implemented control measures to mitigate identified ML risks.

Overall, the sectorial vulnerability rating of this sector is rated as medium, primarily owing to the vulnerability mitigating factors being partially effective.

12.2. Risk Factors

a) **Sales/product base:** Under this category, the FIC took into consideration the casinos' 2017 annual sales. Total sales turnover for the period was NAD 241 636 325.00 for all 5 registered casinos.

   Overall, the exercise assessed the sector's vulnerabilities at a weighted rating of 2.00. Factors such as: large volumes of sales, portion of sales financed by cash and involvement of foreign nationals contributed to this rating.

b) Geographic risk: The sector's risk weighted rating of 2.87 was arrived at owing to the moderate number of foreign nationals using Casino services.

c) Type of client/customer base: The issue of beneficial ownership does not arise amongst the casino clientele, other than at licensing of entity (market entry). However, a moderate rating of 2.60 was noted on this category due to a combination of natural persons and a moderate presence of foreign clients within the sector.

d) Supervisory Bodies & Market entry: In the near future, when the Gaming and Entertainment Control Act of 2018 comes into effect, such Act will present an avenue for The Gaming Control Division (responsible for licensing, and approval of market entry for the Casino sector) to conduct the necessary due diligence required in the AML/CFT sphere. The effectiveness of such measures could not be verified at this stage. Additionally, the Centre, at present could not get assurance that the Gaming Control Division has a process in place to detect any breaches and if such leads to suspensions and cancellations of licenses. Market entry challenges are apparent as far as AML/CFT is concerned. The Casino sector is therefore perceived to be exposed to

higher ML risks. The Casino sector is supervised by the FIC for ML purposes as per Schedule 1 of the FIA. The actual implementation of relevant internal controls to mitigate ML/TF risks by clients in Casinos is, to a certain extent, monitored and measures are taken to help Casinos reduce risk exposure. The overall consideration of these factors resulted in a lower risk rating of 2.

e) **Payment methods:** Collectively, the AML vulnerable exposure due to all payment methods available to the sector, has a vulnerability weighted score of 3.17. Mainly, this is because Casinos are cash intensive institutions, although lately it has been observed that the sector is moving away from cash to other methods of payment such as debit cards as interpreted here below:

- **Cash payment:** On average, 37% of clients in the sector use this method of payment to brings funds into casinos establishments.
- **Electronic Fund Transfers (EFTs):** Only two (from the 5 casinos) used this type of method. The first casino indicated that 33% of funds it received was through EFTs while the second casino indicated that only 10% of funds received was via EFTs.
- **Debit Cards:** On average 31.8% of clients make use of this type of method, out of all five casinos.
- **Credit Cards:** The Sector indicated that 22.6% of clients in casinos use this type of method.

12.3. Vulnerability Mitigating Factors/ Controls

The overall score per this category of analysis is 2.85, indicating that the sector is partially compliant. To a certain extent, Casinos have controls in place to mitigate risks, or the controls are not implemented effectively or consistently. This is owing to a 100% assessment coverage rate within the sector consisting of numerous Onsite and Offsite activities, trainings, awareness sessions, and related sectoral engagements.

12.4. Vulnerability assessment results per sector and per AI

The Casino sector's overall vulnerability classification is **medium to high**, i.e. 3.23 as per the vulnerability calculation. This score is partly attributed to the inherent vulnerability observed in the sector. Secondly, the mitigating controls prevalent in the sector contributed to the residual vulnerability.

OVERALL VULNERABILITY CALCULATION - CASINO SECTOR		Vulnerability weight	Weighted score	
STRUCTURAL VULNERABILITIES				***40%***
Supervisory Body	30%	2.00	**0.60**	
Authority to enter Industry	70%	5.00	**3.50**	
Total Structural Vulnerability	100%	**7.00**		
Average Structural Vulnerability		**3.50**	**4.10**	
Business (inherent) Vulnerability				***60%***
Total Sales/Product Base Vulnerability Exposure	20%	2.00	**0.40**	
Geographic Region Vulnerability	20%	2.87	**0.57**	
Customer Base Vulnerability	30%	2.60	**0.78**	
Delivery Channel Vulnerability	30%	3.17	**0.95**	
Total inherent Vulnerability	100%	**10.6**		
Weighted average inherent Vulnerability		**2.66**	**2.70**	
Vulnerability Mitigants				
Policies and procedures	30%	0.00	**0.00**	
Compliance Officer	5%	0.90	**0.01**	
Training	10%	0.75	**0.01**	
Reporting of STRs and CTRs	20%	0.30	**0.01**	
Aware of FIA obligations	15%	0.15	**0.00**	
In contact with FIC i.e. Training	10%	0.75	**0.01**	
Independent check- internal and external audit	10%	0.00	**0.00**	
Total Vulnerability Mitigants	100%	**2.85**		
Average Vulnerability Mitigants		**0.41**	0.04	
Overall Residual Vulnerability		**3.22**		

Table 23: Overall vulnerability rating for the Casino Sector

Equally, the individual Casino scores within the sector where considered to arrive at the final vulnerability rating. Vulnerability rating of respective casinos in this category ranges from medium to high, i.e., with the lowest being 2.98 and highest being 3.64 respectively.

Entity	Rating
Casino 1	3.63
Casino 2	3.39
Casino 3	3.15
Casino 4	2.98
Casino 5	2.98

Table 24: Individual Vulnerability rating for each Casino Institution

Controls relating to inadequate implementation of policies and procedures, non-reporting of STRs and CTRs and the absence of independent audit reviews on FIA controls across the sector contributed to the rating.

a. The ability of casinos to understand and respond to the request for information effectively and timely. This could be partly attributed to the fact that a briefing session was not held prior to the project commencement by the FIC to contextualize the intent and importance of the exercise;
b. The late submission of questionnaires and non-response of the casinos resulted in significant delays and as a result has impacted the timeliness of the project. Follow-ups and new deadlines had to be reset and agreed with the participants. The cooperation of casinos and the ability to adjust to changing circumstances were vital to the eventual completion of the project, albeit beyond the projected completion date;
c. Although project timelines were provided for in the Project Charter, the time required for the project was underestimated (not realistic) as it did not take into consideration the mentioned constraints.

13. Real Estate Agencies Sector

13.1. Real Estate Agencies Sector Overview

Real Estate Agents (REAs) provide services that are generally vulnerable to potential ML abuse. The opportunity for ML in this sector occurs where the purchases of properties are paid in cash (e.g. not financed through mortgage bonds, loans etc.) and the source of such funds cannot be readily established.

The analysis found that the overall ML vulnerability level in the sector is Low-to-Medium with a rating of 2.13. Some of the factors favorably reducing vulnerability is reduction in the number of cash transactions observed in recent years and the fact that most clients are Namibians whose identification can be readily established. Furthermore, recent trends indicate that estate agents hardly accept cash directly from clients. All funds are usually placed in the trust accounts of Conveyancing Attorneys. Such attorneys would under normal circumstances make payments to all involved parties after conducting

the necessary due diligence in terms of the FIA. This has reduced the volume of cash movements in the sector.

The sector comprises over 300 agencies and 750 agents registered with Namibia Estate Agents Board as the prudential regulator. Based on the data received from the sector, the FIC observed that over 80 percent of the finances flow through 28 percent of the entities. Observations indicated that the industry facilitates funds in excess of NAD 2 billion annually.

13.2. Risk Factors

a) Sales/product base

The weighted vulnerability rating in this regard was 1.03 which falls within the low vulnerability level. This was attributed to the fact that although REAs facilitate highly vulnerability transactions, 90% of the REAs' total sales are low in value. The estimated total sales facilitated by REAs for the period under review amounts to NAD 2,052,689,683[26].

b) Analysis by client geographic risk

The weighted vulnerability exposure for this sector, in terms of this evaluation category is 2.64 (low-to-medium). This was mainly because REAs that have a higher percentage of the market share have a combination of clients that are Namibian and non-Namibian.

c) Analysis by type of client/customer base

The weighted vulnerability rating of 2.79 was arrived at as most REAs have a combination of legal and natural persons as their clients.

d) Role of Supervisory Bodies & Authority to enter the Market

This sector's regulatory body is the Namibia Estate Agents Board. However, the Namibia Estate Agents Board does not conduct fit and proper assessments on beneficial owners and directors.

[26] FIC estimates

This, together with other considerations resulted in a weighted vulnerability rating of 2.11 per this category.

e) Analysis by payment method

- **Cash Payments:** The sector indicated that on average, only 3 percent of their transactions are paid in cash;
- **Electronic Funds Transfers (EFT):** The sector indicated that on average, 32 percent of their clients make use of EFT as a method of payment;
- **Debit or Credit Cards:** The sector has no clients using this payment method;
- **Cheque payments:** Prior to the ceasing of cheques, only 0.1 percent of clients in this sector used cheque payments.
- **Bank financing:** The sector indicated that on average, about 65 percent of clients use this method of financing their properties. With bank financing, the risk is inherently lower.

13.3. Vulnerability Mitigating Factors/ Controls

As per the analysis, the overall score of this sector in terms of control implementation is 0.86, indicating that the sector is partially compliant. Some REAs do not have adequate controls in place to mitigate vulnerabilities, or the controls are not implemented effectively.

13.4. Vulnerability assessment per Sector

The sector's overall vulnerability rating is low-to-medium, with an average rating of 2.13 as per the methodology employed. See the below table for detailed scoring and analysis outcomes.

OVERALL VULNERABILITY CALCULATION - REAL ESTATE AGENTS		Vulnerability weight	Weighted score	
STRUCTURAL VULNERABILITY				***40%***
Supervisory Body	30%	2.11	**0.63**	
Authority to enter Industry	70%	1.97	**1.38**	
Total Structural Vulnerability	100%	**4.09**		
Average Structural Vulnerability		**2.04**	**2.02**	
Business (inherent) vulnerability				***60%***
Total Sales/Product Base vulnerability Exposure	20%	1.03	**0.21**	
Geographic Region vulnerability	20%	2.64	**0.53**	
Customer Base vulnerability	30%	2.79	**0.84**	
Delivery Channel vulnerability	30%	2.66	**0.80**	
Total inherent vulnerability	100%	**9.1**		
Weighted average inherent vulnerability		**2.28**	**2.37**	
Vulnerability Mitigants				
Policies and procedures	25%	0.80	**0.03**	
Compliance Officer	5%	1.51	**0.01**	
Training	10%	0.76	**0.01**	
Reporting of STRs and CTRs	15%	0.37	**0.01**	
Aware of FIA obligations	15%	1.35	**0.03**	
In conduct with FIC i.e. Training	5%	0.97	**0.01**	
Independent check- internal and external audit	10%	0.27	**0.00**	
Total Vulnerability Mitigants	85%	**6.03**		
Average Vulnerability Mitigants		**0.86**	0.10	
Overall Residual Vulnerability		**2.13**		

Table 25: Overall vulnerability rating for the Real Estate Agencies Sector

The rating of individual REA within the sector ranges from low-to-medium, i.e. lowest being 1.75 and highest being 2.69 respectively. The analysis considered the different implementation and effectiveness levels of internal ML control frameworks in each individual institution.

Institution	Risk Rating		Institution	Risk Rating
REA 1	2.7		REA 38	2.1
REA 2	2.5		REA 39	2.1
REA 3	2.5		REA 40	2.1
REA 4	2.5		REA 41	2.1
REA 5	2.5		REA 42	2.1
REA 6	2.5		REA 43	2.1
REA 7	2.5		REA 44	2.1
REA 8	2.5		REA 45	2.0
REA 9	2.5		REA 46	2.0
REA 10	2.5		REA 47	2.0
REA 11	2.4		REA 48	2.0
REA 12	2.4		REA 49	2.0
REA 13	2.4		REA 50	1.9
REA 14	2.4		REA 51	1.9
REA 15	2.4		REA 52	1.9
REA 16	2.4		REA 53	1.9
REA 17	2.4		REA 54	1.9
REA 18	2.4		REA 55	1.9
REA 19	2.4		REA 56	1.9
REA 20	2.3		REA 57	1.9
REA 21	2.3		REA 58	2.2
REA 22	2.3		REA 59	1.9
REA 23	2.3		REA 60	1.9
REA 24	2.3		REA 61	1.9
REA 25	2.2		REA 62	1.9
REA 26	2.2		REA 63	1.9
REA 27	2.2		REA 64	1.9
REA 28	2.2		REA 65	1.9
REA 29	2.2		REA 66	1.9
REA 30	2.2		REA 67	1.9
REA 31	2.2		REA 68	1.9
REA 32	2.2		REA 69	1.9
REA 33	2.2		REA 70	1.9
REA 34	2.2		REA 71	1.9
REA 35	2.1		REA 72	1.9
REA 36	2.1		REA 73	1.9
REA 37	2.1		REA 74	1.7

Table 26: Overall vulnerability rating for the Real Estate Agencies

14. Banking Sector

14.1. Banking Sector Overview

The sector comprises 9 entities/banks. As part of this exercise, the FIC observed that over 98% of deposits (electronic and cash) flows through 33% of the entities which are considered the largest in the sector. In terms of remittances, the four largest banks account for 88% of the inward and 95% of outward remittances.

Observations indicate that the industry has annual deposits of over NAD 400 billion.[27]

Deposit taking services, cross border remittances, lending services and foreign exchange services are but some of the services which expose the financial system to potential ML risks. The ability of clients transacting with different persons via the banking systems also enhance ML vulnerability.

14.2. Risk Factors

a) Analysis by geographic risk

The rationale is that local banks may not always be in a position to readily verify the authenticity of client's identification and relevant particulars, thus compromising the CDD effectiveness. Banks that have clients from other jurisdictions expose the national financial system to vulnerability levels greater than others. They are thus rated higher in this category.

The rating for the sector in this category indicates that banks have more Namibian clients compared to other nationals and have limited services provided outside the country without adequate mitigating controls.

b) Analysis by the type of client/customer base

Clients who are legal persons inherently present higher ML risk than natural persons when the ultimate beneficial owners in such legal persons cannot be readily and reliably identified. Inherently, the more legal persons a bank has as clients, the higher its ML vulnerability. Vulnerability in terms of this factor was considered along these lines.

It is perceived that beneficial owners who may launder proceeds of crime will most likely use complex ownership structures that hide their identification or representation. From the FIA compliance assessment activities conducted in the sector, the FIC observed that in most cases, beneficial owners' information was not adequately obtained when business relationships were established.

c) Analysis of deposit takings

[27] FIC data collected from the Sector

The analysis of deposit taking took into account the values and transaction volumes of deposits at each banking institution in comparison to the sector. Banks with higher transactional volumes and values are perceived to have a higher vulnerability level (inherently) than others with lower volumes and values.

The analysis further included reviews of the methods of deposits employed e.g. cash or EFTs, etc. Accordingly, a progressive rating was allocated to cash deposits based on the percentage of total deposits while a regressive rating was allocated to other forms of payments as they are perceived to have less vulnerability exposure. This basically means the more cash deposits a bank received the higher the inherent vulnerability rating. In the same vein, the more EFT and other forms of payments a bank received, the lower the vulnerability rating assigned. Further, the analyses took into account the volumes of transactions (values and volumes) conducted by individuals and legal persons. Legal persons, especially ones whose ultimate beneficial owners cannot be readily identified present a higher ML risk.

Accordingly, the sector has a high weighted vulnerability rating derived from an assessment of the above factors.

d) Foreign exchange services

Banks are part of the authorized dealers in foreign currencies in terms of the Currencies and Exchanges Act, Act No. 9 of 1933. The currency exchange services are inherently vulnerable to potential abuse for money laundering. A few examples include exchanging large amounts of cash, clients structuring transactions over time in one or more institutions etc.

The higher transfer speed and the cash intensive nature of currency exchange services escalate their attractiveness to ML activities. The analysis of this section took into account the transaction volumes and values in different currencies for each bank in relation to the sector. Additionally, the analysis took into account the methods used in exchanging the currency i.e. exchanges in cash or from bank accounts.

It should further be noted that not all the banks offer this service although the four biggest banks offer almost all types of banking services.

e) Analysis of cross border remittance services

The growth in the global economy has made international trade an increasingly attractive avenue to move illicit funds through financial transactions associated with the international trade in goods and services[28]. The banking and other sectors involved in the remittance of funds for different purposes to different jurisdictions across the globe are exposed to the risk of Trade Based Money Laundering (TBML) amongst other risks that come with international trade. Namibia, being part of the global economy is not immune to the abuse of the financial system through international trade and the ongoing trial in which funds exceeding NAD 4 billion could have been laundered through potential irregular customs practices is a prime example of such national vulnerability. The FIC Guidance Note No. 02 of 2017[29], and the studies cited in that document highlight such vulnerability in the banking sector.

Launderers have also been abusing the Balance of Payment (BoP) categories, particularly those were less supporting information is required for cross border remittances (e.g. gift remittances). Given the inadequate control in the banking system and related sectors, persons there has been significant abuse of the remittances services augmented by indicators such as the remittances of funds in excess of prescribed limits, failures to present supporting documents to financial institutions. The manipulation of invoices with the intention to remit more funds is one of the common methods used to launder proceeds through cross border remittances.

f) Analysis of lending services

The analysis under this section was based on the view that the ML vulnerability exposure for lending services is mostly with the settlement of loans earlier than their maturity dates or clients merely using proceeds from illicit activities to settle legitimate loans. The movement of balances on the loan account with significant percentages higher than the expected reduction as per expected repayments can indicate the likelihood with which lending can be susceptible to ML exposure.

g) Analysis of nationalities from high risk jurisdictions or jurisdictions not known to have adequate AML/CFT/CPF controls in place

The FATF and the United Nations lists certain jurisdictions that have not met international standards geared towards combatting ML/TF/PF activities. The analysis of this section took into account the

[28]APG Typology Report on Trade Based Money Laundering, Adopted by APG Members at the 15th Annual Meeting 20 July 2012
[29] Available on the FIC website

relevant exposures emanating from engaging clients from such jurisdictions or those remitting funds to and from such jurisdictions. The relationship of the client to the destinations where funds are remitted to or from as well as involved financial values and frequency were considered.

h) Business inherent vulnerability

The weighted average business inherent vulnerability exposure for the sector was rated at 3.83. This rating indicates that the banking sector is more vulnerable considering its type of clients, products and services, method of payments and the geographic area of its clients.

14.3. Vulnerability mitigating factors/controls

The overall score for this sector in terms of control implementation was rated at 1.04. This rating indicates that the sector has relatively fair controls in place. The sector therefore remains vulnerable in as far as expected controls are not at a level they should be.

14.4. Vulnerability assessment results per sector

The sector's overall vulnerability rating is "Medium-High". It was calculated at an average of 3.78 as per the methodology employed. *Refer to the table below.*

OVERALL VULNERABILITY CALCULATION		Risk weight	Weighted score	
STRUCTURAL VULNERABILITY				*40%*
Supervisory Body	30%	4.00	**1.20**	
Authority to enter Industry	70%	4.00	**2.80**	
Total Structural Risk	100%	**8.00**		
Average Structural Risk		**4.00**	**4.00**	
Business (inherent) Vulnerability				*60%*
Geographic Region	15%	4.85	**0.73**	
Customer Base	10%	4.94	**0.49**	
Deposit Taking	15%	4.89	**0.73**	
Type of Clients	10%	3.90	**0.39**	
Foreign Exchange Services	10%	2.46	**0.25**	
Cross Border Remittance Services	15%	3.16	**0.47**	
Lending Services	10%	3.98	**0.40**	
Nationalities From Certain FATF Listed Countries	15%	2.43	**0.36**	
Total inherent risk	100%	**30.6**		
Weighted average inherent risk		**3.83**	**3.83**	
Risk Mitigants				
Policies and procedures	25%	0.75	**0.02**	
Compliance Officer	5%	1.50	**0.01**	
Training	5%	1.33	**0.01**	
Reporting of STRs and CTRs	20%	0.67	**0.02**	
Aware of FIA obligations	10%	1.25	**0.02**	
In conduct with FIC i.e. Training	10%	1.08	**0.01**	
Sanction Screening controls	15%	0.83	**0.02**	
Independent check- internal and external audit	10%	0.92	**0.01**	
Total Risk Mitigants	100%	**8.33**		
Average Risk Mitigants		**1.04**	0.11	
Overall Residual Risk		**3.78**		

Table 27: Overall vulnerability rating for the Banking Sector

The table below indicates the ratings for the individual banks.

Banking Sector Vulnerability Rating	
Name of Entity	**Rating**
Bank 1	3.97
Bank 2	4.01
Bank 3	3.07
Bank 4	3.64
Bank 5	4.27
Bank 6	2.73
Bank 7	4.15
Bank 8	3.62
Bank 9	2.47

Table 28: Individual vulnerability rating of banks

15. Motor Vehicle Dealership Sector

15.1. Motor Vehicle Dealership Sector Overview

Motor Vehicle Dealers provide services that are generally perceived as services highly vulnerable to potential ML threats. Entities in this sector are frequently visited by customers and can be exploited through the purchasing of motor vehicles in order to disguise the origin of proceeds of illicit activities.

Generally, the buying and selling of motor vehicles can be used as a platform for Money Laundering, Terrorism and Proliferation Financing activities. Within our jurisdiction the Money Laundering risk is higher than Terrorism and Proliferation Financing risk. The most obvious manner to launder funds through the sector is the usage of proceeds from illicit activities to fund vehicle purchases. In the same vein, vehicles that were initially sourced with proceeds of crime can be sold and the funds thereof layered through the financial system. These activities can undermine the integrity of our financial system.

The sector comprises of about 520 entities[30], however only 89 entities are registered with the FIC. As part of this exercise, the FIC observed that over 89% of finances flow through 35% of entities which are considered the largest in the sector.

Observations indicate that the industry's annual revenues exceed NAD 4 billion.

15.2. Risk Factors

a) Analysis by Sales/product base

The overall risk weight was recorded at 1.24.

b) Analysis by client Geographic risk

The weighted vulnerability rating in terms of this factor was recorded as 2.16. The low–medium rating was attributed to a fair presence of foreign clients amongst the sectors' clientele.

c) Analysis by Type of client/customer base

A medium to high weighted vulnerability rating of 3.50 is allocated to the MVDs sector in this regard. The majority of MVDs were observed to have a combination of legal and natural persons and a foreign client base.

d) Role of Supervisory Bodies & Authority to enter the Market

Market entry in the sector is relatively easy as there are no entry controls. Most dealers simply registered businesses with the Registrar of Companies. There are no regulatory due diligence controls on ultimate beneficial owners prior to market entry. Due to reasons given above, the MVDs sectors' weighted vulnerability rating in this category was calculated at 5.

e) Analysis by Payment methods

- **Cash payment:** The sector indicated that on average, only 5 percent of their transactions are paid in cash;

[30] Data from NATIS systems

- **Electronic Funds Transfer (EFT):** The sector indicated that on average 36 percent of their clients make use of EFT as a method of payment;
- **Debit or Credit Cards:** The sector has no clients using this payment method;
- **Bank Financing:** The sector indicated that on average, about 59 percent of clients use this method of financing their properties.

Accordingly, this sector has a weighted score of 2.57 per this category owing to the fact that most MVSs' sales are bank financed.

15.3. Vulnerability Mitigating Factors/ Controls

As per the analysis, the overall score for this sector in terms of control implementation was scored at 1.07. This rating indicates that the sector/MVDs have relatively fair controls in place and/or the ineffective implementation thereof. The sector therefore remains exposed to a certain level of vulnerability.

15.4. Vulnerability assessment results per sector

The sector's overall vulnerability classification is "Medium-High". It was calculated at an average of 3.38 as per the methodology employed. *Refer to the table below.*

OVERALL VULNERABILITY CALCULATION - MOTOR VEHICLE DEALERS		Risk weight	Weighted score		
STRUCTURAL RISKS					***40%***
Supervisory Body	30%	4.82	**1.45**		
Authority to enter Industry	70%	5.00	**3.50**		
Total Structural Risk	100%	**9.82**			
Average Structural Risk		**4.91**	**4.95**		
Business (inherent) Risk					***60%***
Total Sales/Product Base Risk Exposure	20%	1.24	**0.25**		
Geographic Region Risk	20%	2.16	**0.43**		
Customer Base Risk	30%	3.50	**1.05**		
Delivery Channel Risk	30%	2.79	**0.84**		
Total inherent risk	100%	**9.7**			
Weighted average inherent risk		**2.42**	**2.57**		
Risk Mitigants					
Policies and procedures	30%	0.93	**0.04**		
Compliance Officer	5%	1.50	**0.01**		
Training	10%	1.06	**0.02**		
Reporting of STRs and CTRs	20%	0.75	**0.02**		
Aware of FIA obligations	15%	1.32	**0.03**		
In conduct with FIC i.e. Training	10%	1.41	**0.02**		
Independent check- internal and external audit	10%	0.53	**0.01**		
Total Risk Mitigants	100%	**7.50**			
Average Risk Mitigants		**1.07**	0.14		
Overall Residual Risk		**3.38**			

Table 29: Overall vulnerability rating for the Motor Vehicle Dealership Sector

The assessment analysis on individual vulnerability to ML is summed up herein. The rating scores of individual MVDs ranged from “medium” to “medium-high”. The lowest a lowest rated MVD scored 2.95 while the and highest scored 3.78 respectively. The analysis considered the different implementation and effectiveness levels of internal ML control frameworks in each individual institution.

No	Entity	Rating
1	MVD1	3.83
2	MVD2	3.78
3	MVD3	3.59
4	MVD4	3.52
5	MVD5	3.49
6	MVD6	3.46
7	MVD7	3.46
8	MVD8	3.39
9	MVD9	3.39
10	MVD10	3.30
11	MVD11	3.26
12	MVD12	3.22
13	MVD13	3.22
14	MVD14	3.20
15	MVD15	3.19
16	MVD16	3.13
17	MVD17	2.95

Table 30: Motor vehicle Dealer Individual Vulnerability ratings

16. Authorized Dealers with Limited Authority (ADLAS)Sector

16.1. ADLAS Sector Overview

The ADLAs sector comprises eight registered entities. In terms of institutional size, the table below is indicative of each entity’s revenue and asset base in the period reviewed:

Name of the Institution	Revenue (NAD)	Profit after Tax (NAD)	Assets (NAD)
A	323,948	(332,318)	1,914,414
B	17,878,707	(687,624)	398,510

C	6,701,704	(1,146,263)	3,448,251
D	2,880,869	507,556	2,054,744
E	*No Data*	*No Data*	*No Data*
F	12,133,511	2,598,244	13,711,810
F	18,102,156	4,709,645	13,510,063
G	411,166	(1,314,020)	4,228,713
TOTAL	**58,432,061**	**4,335,220**	**39,266,505**

Table 31: ADLAs Annual Financial Statements from Bank of Namibia (Source: Exchange Control Department)

The total financial assets of the ADLAs sector is around NAD 40 million.

16.2. Risk Factors

a) Analysis by product/service base

The weighted vulnerability rating for this factor is 2.60.

b) Analysis by Geographic Risk

The weighted vulnerability rate for this factor is 3.13. This is a medium rating. Generally, the imbedded AML controls arising from agreements between different remitting agencies give assurance that partnering agencies through cross border remittances have reasonable control measures in place to reduce inherent risks.

c) Analysis by the type of client/customer base

The weighted vulnerability exposure for this sector is 3.30 for this category, as most ADLAs could have a combination of both legal and natural persons as their clients.

d) Supervisory bodies and authority to enter the market

The vulnerability score of this category was 2.80 or low-medium.

e) Foreign currency exchange services

The sector has a weighted rating of 2.08, attributed to the exposure of these services and the volumes of transactions in the sector.

f) Cross border remittance services

The assessment noted that despite abuses observed in other sectors of this factor, the transactional values are often very low and this, amongst others led to the lower ratings of 1.74.

g) Cross Border remittances by NPOs

Given the exposure associated with ADLAs dealing with NPOs and the value of transactions remitted, the risk rated for this service is 0. This is because the ADLAs conducts non-trading related transactions which are mostly with natural persons. Therefore, transactions involving organizations are highly unusual. Whatever risk there maybe can stem from natural persons remitting or receiving funds on behalf of NPOs and such is not declared or known by ADLAs.

h) High risk jurisdictions in terms of ML/TF/PF risks

The sector has a weighted rating of 2.16, attributed to the exposure of dealing with individuals from these jurisdictions and the volumes and values of transactions in the sector.

16.3. Vulnerability mitigating factors/controls

As per the analysis, the sector attained an overall rating of 1.05, indicating that the sector is partially compliant.

16.4. Vulnerability assessment results for the sector

The sector's overall vulnerability classification is Medium, with an overall rating of 2.18 as per the risk calculation (see table below). This score is mainly attributed by the inherent risk as observed in the sector. However, the mitigating controls prevalent in the sector reduces the inherent vulnerability.

OVERALL VULNERABILITY CALCULATION		Risk weight	Weighted score		
STRUCTURAL RISKS					*40%*
Supervisory Body	30%	2.80	**0.84**		
Authority to enter Industry	70%	2.80	**1.96**		
Total Structural Vulnerability	100%	**5.60**			
Average Structural Vulnerability		**2.80**	**2.80**		
Business (inherent) Vulnerability					*60%*
Total Sales/Product Base Vulnerability Exposure	10%	2.60	**0.26**		
Geographic Region Vulnerability	15%	3.13	**0.47**		
Customer Base Vulnerability	15%	3.30	**0.50**		
Foreign Exchange Services	10%	2.08	**0.21**		
Analysis Of Cross Border Remittance Services	15%	1.74	**0.26**		
Cross Border Remittances By NPOs	20%	0.00	**0.00**		
Nationalities From Certain FATF Listed Countries	15%	2.16	**0.32**		
Total inherent Vulnerability	100%	**15.0**			
Weighted average inherent Vulnerability		**3.75**	**2.02**		
Vulnerability Mitigants					
Policies and procedures	30%	1.05	**0.05**		
Compliance Officer	10%	1.05	**0.02**		
Training	10%	1.05	**0.02**		
Reporting of STRs and CTRs	15%	1.05	**0.02**		
Aware of FIA obligations	15%	1.05	**0.02**		
In conduct with FIC i.e. Training	10%	1.05	**0.02**		
Independent check- internal and external audit	10%	1.05	**0.02**		
Total Vulnerability Mitigants	100%	**7.35**			
Average Vulnerability Mitigants		**1.05**	0.15		
Overall Residual Vulnerability		**2.18**			

Table 32: Overall vulnerability rating for the ADLAS Sector

It is worth noting that the scores of respective ADLAs within the sector range from Medium to Medium-High. Refer to table 33 below.

No	Institutions	Risk Ratings
1	A	2.89
2	B	2.81
3	C	2.72
4	D	2.67
5	E	2.65
6	F	2.60
7	G	2.55

Table 33: ADLAs Individual Vulnerability Ratings

17. Accountants and Auditors Sector

17.1. Accountants and Auditors Sector Overview

The Public Accountants and Auditors' Board, established in terms of the Public Accountants and Auditors' Act, 1951 (Act No. 51 of 1951) supervises and regulates Accountants and Auditors in Namibia

for prudential purposes. To date there are 56 Institutions which are auditing firms registered by PAAB for supervision. The rest of the other accountants are members of other professional bodies. The Institute of Chartered Accountants in Namibia (ICAN) has only individual membership with no Institutions as members while others such as the Namibian Institute for Professional Accountants (NIPA) comprises individual members and 15 Institutions which are Accounting firms and the Southern Africa Institute for Business Accountants (SAIBA) comprises of only individual members with no Institutions membership.

The FIC could not find reliable estimation of industry size in terms of annual revenues generated by the sector. However, it could be estimated that the small to medium sized institution in this sector could generate up to NAD 2,000,000.00 in annual sales. The medium to larger sized institutions is said to generate much more than that depending on the size, nature, volume and type of clients they serve.

17.2. Risk Factors

a) Analysis by product/service base

Similar to the other sectors, the analysis of products/services also considered the percentage of Accountants' total sales in comparison to the sectoral totals. Accountants with higher sales percentages are perceived to be inherently more exposed to risks (Likelihood), hence the rating allocation (Impact) is higher than Accountants with lower sales percentages. The weighted vulnerability rating for this factor is 1.08.

b) Analysis by geographic risk

The weighted risk rate for this factor is 1.16. This relatively lower rating is informed by the significantly low number of foreign clients serviced by Accountants.

c) Analysis by the type of client/customer base

The weighted vulnerability exposure for this category is thus 2.47.

d) Supervisory bodies and authority to enter the market

Part of this sector with the auditing function is regulated by the Public Auditors and Accountants Board (PAAB) and the rest of the accountants are members of professional institutes such as ICAN, NIPA and SAIBA. The FIC remains the primary AML supervisor while the said professional bodies and the PAAB are entrusted with prudential regulation responsibilities. Consideration of these factors resulted in a lower vulnerability rating. Accordingly, the vulnerability score for this category was 2.08.

e) Analysis by payment method

In terms of the methodology employed, the below should be noted:

- **Cash payments:** The percentage of payment volumes in the sector via cash is 1.62%;
- **Electronic Funds Transfers (EFTs):** The percentage of payment volumes in the sector via the EFT payment channel is 96%;
- **Debit and credit cards:** The percentage of payment volumes in the sector via Debit and credit card payment channel is 0.82%;
- **Cheque payments:** The percentage of payment volumes in the sector via cheque payment channel is 1.71%. However, the payment method has since been discontinued and therefore no longer presents ML/TF/PF risks to the country.

17.3. Vulnerability mitigating factors/controls

As per the analysis, the sector attained an overall score of 0.60, indicating that the sector is partially compliant. As evidenced from the compliance assessments, some Accountants do not have adequate controls in place to mitigate vulnerability, or the controls are not implemented effectively.

17.4. Vulnerability assessment results for the sector

In summary, the sector's overall vulnerability classification is low to medium, i.e. 1.86 as per the risk calculation, in terms of the methodology employed.

OVERALL RISK CALCULATION - ACCOUNTANTS & TRUST AND COMPANY SERVICE PROVIDERS		Risk weight	Weighted score		
STRUCTURAL RISKS					*40%*
Supervisory Body	30%	2.08	**0.62**		
Authority to enter Industry	70%	2.68	**1.88**		
Total Structural Risk	100%	**4.76**			
Average Structural Risk		**2.38**	**2.50**		
Business (inherent) Risk					*60%*
Total Sales/Product Base Risk Exposure	20%	1.08	**0.22**		
Geographic Region Risk	20%	1.16	**0.23**		
Customer Base Risk	30%	2.47	**0.74**		
Delivery Channel Risk	30%	1.30	**0.39**		
Total inherent risk	100%	**6.0**			
Weighted average inherent risk		**1.50**	**1.58**		
Risk Mitigants					
Policies and procedures	30%	0.65	**0.03**		
Compliance Officer	10%	0.55	**0.01**		
Training	10%	0.65	**0.01**		
Reporting of STRs and CTRs	15%	0.65	**0.01**		
Aware of FIA obligations	15%	0.63	**0.01**		
In conduct with FIC i.e. Training	10%	0.39	**0.01**		
Independent check- internal and external audit	10%	0.65	**0.01**		
Total Risk Mitigants	100%	**4.18**			
Average Risk Mitigants		**0.60**	0.09		
Overall Residual Risk		**1.86**			

Table 34: Overall vulnerability rating for the Accountants and Auditors Sector

18. Conclusion

The observations and outcomes of this assessment will be used to inform enhance the overall AML/CFT/CPF framework. Amongst others, these outcomes will enhance the current risk based approach employed in supervisory activities.

Arriving at a risk position is informed by the level of threats and sectoral vulnerabilities. This assessment found the sectoral vulnerability to be **Medium (2.82)** while threats were rated as **High**, thus arriving at the overall level of **Medium High**.

The norm is that all sectors assessed as presenting a high vulnerability rating are reviewed every 12 to 24 months, depending on circumstances. Given the medium-high rating, it is anticipated that the next SVA updates for the Banking and CCFAs sectors would be undertaken within the next 36-48 months from the date of finalizing this study, wit due consideration to the outcomes of the NRA activity taking place in 2020.

K.H Hamutenya

Deputy Director: Compliance Monitoring and Supervision