

ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM SECTOR RISK ASSESSMENT OF

**AUTHORISED USERS OF AN EXCHANGE
COLLECTIVE INVESTMENT SCHEMES MANAGERS
FINANCIAL SERVICES PROVIDERS**

ISSUED BY THE FINANCIAL SECTOR CONDUCT AUTHORITY

MAY 2019

TABLE OF CONTENTS

Glossary	3
Executive Summary	5
Background and purpose of the Sector Risk Assessment	8
Methodology	10
Criminal Threats	13
Vulnerabilities	19
Consequences	34

GLOSSARY

AI	Accountable institutions referred to in items 4, 5 and 12 of Schedule 1 to the FIC Act.
AML	Anti-money laundering
AML/CFT	Anti-money laundering and/or the combatting of financing of terrorism
AUTHORISED USER	Authorised user of an exchange
CIS	Collective Investment Scheme
CISCA	Collective Investment Schemes Control Act, No 45 of 2002
CIS Manager	Collective Investment Schemes Manager
CTR	Cash threshold report(ing)
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FAIS Act	Financial Advisory and Intermediary Services Act, No. 37 of 2002
FATF	Financial Action Task Force
FIC Act	Financial Intelligence Centre Act, No. 38 of 2001
FMA	Financial Markets Act, 2004
FSCA	Financial Sector Conduct Authority
FSP	Financial services provider
LISP	Linked investment service provider

ML/TF	Money laundering and/or terrorist financing
NGO	Non-government organization
NPO	Non-profit organization
PEP	Politically exposed person
STR	Suspicious transaction report(ing) and suspicious activity report(ing)
TF	Terrorist Financing
TPR	Terrorist Financing Report
FIC	Financial Intelligence Centre

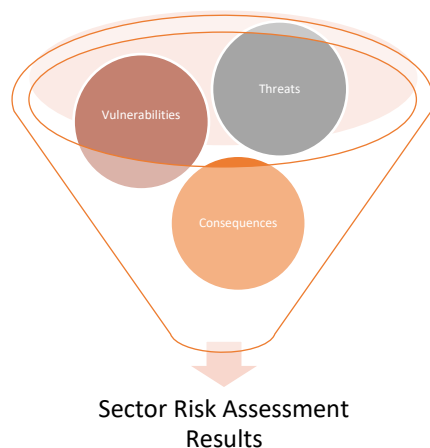
A. EXECUTIVE SUMMARY

The FSCA is responsible to supervise three sectors for compliance with the FIC Act namely:

- Authorised users;
- CIS Managers; and
- FSPs (Note: FSPs are broken down into sub-categories of Financial advisers & Intermediaries, Investment managers, Hedge fund managers and LISPs)

Below is a summary of the findings of a risk assessment conducted on the above-mentioned sectors in order to understand the ML/TF risks in those sectors. The FSCA assessed the ML/TF risks for a two-year period being 2016/17 and 2017/18 financial years. The assessment focused on money laundering only. The services provided by financial institutions are less likely to facilitate terrorist financing. There is no hard data to suggest that the sector is exposed to TF risk. No TF activities have been identified in the financial sector during onsite & off-site inspections and other interactions. The financial sector has not filed any terrorist property reports.

In conducting the sector risk assessment, the FSCA evaluated three areas namely criminal threats, vulnerabilities and consequences.



Threats

Threats are predicate offences and ML risks to which the financial sector may be exposed. STRs played a key role to determine threats. Threats were determined based on the types of offences reported in the STRs.

The most common reason provided by the three sectors for reporting STRs related to suspicious and/or unusual transactions/activities mentioned in section 29 of the FIC Act.

The most common issues reported in the STRs which point to possible ML threats are:

- Unauthorised business;
- Ponzi schemes;
- Fraud;
- Insider trading; and
- Tax evasion

The financial sector has been assessed as follows from a **threat** perspective:

Authorised users	CIS managers	FSPs			
		Financial advisers & Intermediaries	Investment managers	Hedge fund managers	LISPs
Low	Low	Low	Low	Low	Low

Vulnerabilities

Vulnerabilities are features of the industry that make it attractive for ML purposes. Vulnerabilities were determined based on the results of a questionnaire (completed by Authorised users, CIS Managers & FSPs) and the outcome of onsite and offsite inspections.

There are several features or elements of the businesses in the sector that could be exploited. The following risk factors were considered:

- Clients;
- Products & services;
- Distribution channels;
- Geographic locations.

The financial sector has been assessed as follows from a **vulnerability** perspective:

Authorised users	CIS managers	FSPs			
		Financial advisers & Intermediaries	Investment managers	Hedge fund managers	LISPs
Medium	Low	Low	Medium	Medium	Medium

Consequences

Consequence refers to the impact or harm that ML risks may cause or have on clients, financial institutions, the financial sector and the broader South African economy. The following criteria have been considered to determine consequences:

- Harm or loss to clients;
- Harm or loss to financial institutions;
- Harm or loss to the financial sector; and
- Harm or loss to the South African economy.

The controls put in place by financial institutions in the various sectors regulated by the FSCA will minimise any harm or damage caused by ML risks. The controls largely refer to measures for compliance with the FIC Act.

Overall ML Risk Rating

The overall **threat** and **vulnerability** of the financial sector regulated by the FSCA has been assessed as follows:

Authorised users	CIS managers	FSPs			
		Financial advisers & Intermediaries	Investment managers	Hedge fund managers	LISPs
Medium	Low	Low	Medium	Medium	Medium

B. BACKGROUND

This report sets out the findings of the risk assessment conducted by the FSCA on the sectors regulated and supervised by it for compliance with the AML/CFT laws. The purpose of the risk assessment is to examine the ML/TF threats and vulnerabilities facing these sectors. The FSCA is responsible to supervise the following entities for compliance with the FIC Act:

- An Authorised user as defined in the Financial Markets Act, 2004;
- A CIS Manager registered in terms of the Collective Investment Schemes Control Act, 2002;
- A person who carries on the business of a financial services provider (FSP) authorised or requiring authorisation in terms of the FAIS Act. The FSPs were broken down into sub-categories of Financial advisers & Intermediaries, Investment managers, Hedge fund managers and Linked Investment Service Providers (LISPs).

The sector risk assessment was conducted for the following reasons:

- To inform a risk-based approach to supervision. A risk-based approach to supervision refers to:
 - The general process by which a supervisor, according to its understanding of risks, allocates resources to AML/CFT supervision; and
 - The specific process of supervising institutions that apply an AML/CFT risk-based approach.

This means that a supervisory body should have a clear understanding of the ML/TF risks present in the sectors that it supervises and base the frequency and intensity of on-site and off-site supervisions on such ML/TF risks.

- To assist financial institutions to identify, assess and take effective action to mitigate the ML/TF risks.

C. RISK ASSESSMENT METHODOLOGY

The ML/TF risks were assessed for a two-year period being 2016/17 and 2017/18. Various methods were used to collect data from various sources e.g. consultation with the FIC, review internal records and databases, onsite & off-site inspections, results of the questionnaires, literature review (typologies studies, mutual evaluation reports etc.), as well as guidance issued by the FATF.

The assessment focused on money laundering only. The services provided by financial institutions are less likely to facilitate TF. There is no hard data to suggest that the sector is exposed to TF risk. In conducting the sector risk assessment, three areas were evaluated namely threats, vulnerabilities and consequences.

Threats refer to criminal threats, including ML/TF risks that face the industry. In assessing threats, the following information was considered:

- Number of licensed businesses and individuals;
- Number of STRs, CTRs and TPRs submitted by the industry;
- The types of offences that were reported by the industry;
- Reasons for suspicious transaction / activity reporting; and
- ML trends in the industry.

Vulnerabilities refer to the features of the industry that make it attractive for ML/TF purposes. The following information was considered:

- Clients
 - Types of clients;
 - Prevalence of foreign based clients;
 - Prevalence of high-risk clients such as foreign prominent public officials or domestic prominent influential persons.
- Products
 - Cash intensity;

- Whether products allow clients to remain anonymous;
- Complexity of the products;
- Cross-border transactions;
- Third party payments or deposits;
- Cooling-off periods and refunds.
- Distribution channels
 - Dealings with non-banked, walk-in or occasional clients;
 - Distribution of products through other FSPs, group entities or third parties;
 - Non-face-to-face transacting using telephone or internet.
- Geographies
 - Residence of clients in high risk jurisdictions;
 - Use of intermediaries outside South Africa;
 - Residence of clients in countries with strict secrecy laws.
- Mitigation of ML risks
 - Compliance by the industry with AML/CFT obligations;
 - Systems and controls implemented to mitigate against ML risks;
 - The use of internal audit to review ML risks.

Consequence refers to the impact or harm that ML/TF risks may cause or have on clients, financial institutions, the financial sector and the broader South African economy. The following criteria have been considered to determine consequences:

- Harm or loss to clients;
- Harm or loss to financial institutions;
- Harm or loss to the financial sector; and
- Harm or loss to the South African economy.

The first stage of the risk assessment entailed the process of identification of ML risks. These were drawn from known or suspected threats or vulnerabilities.

- For threats, information relating to STRs filed by Authorised users, CIS Managers and FSPs for the period 2016/17 and 2017/18 was obtained from the FIC. Note that the FIC did not record STRs according to the different types of FSPs. All types of FSPs register and report under item 12 of Schedule 1 to the FIC Act.
- For vulnerabilities, questionnaires were issued to Authorised users, CIS Managers and FSPs. The outcome of onsite and off-site inspections conducted from 2014/15 to 2017/18 were also considered.

The second stage of the risk assessment entailed analysis of the data provided. It involves consideration of the nature, sources, likelihood and consequences of the identified risks. The aim of this stage is to gain a holistic understanding of each risk – as a combination of threats, vulnerabilities and consequences in order to work towards assigning some sort of relative value to each risk. An average risk rating was determined for each risk factor, which was then used to determine an overall risk rating for each sector.

Each sector was then assessed as Low, Medium or High risk. It must be noted that a rating of low risk does not mean that there is no risk within the sector. Money laundering may still take place through low risk sectors. Similarly, a high risk rating is not indicative of a lack of compliance in the sector. Some sectors, by their nature, always have a higher level of inherent risk.

D. OVERALL ML RISK LEVELS

The overall threat and vulnerability of the financial sectors regulated by the FSCA has been assessed as follows:

Authorised users	CIS managers	FSPs			
		Financial advisers & Intermediaries	Investment managers	Hedge fund managers	LISPs
Medium	Low	Low	Medium	Medium	Medium

E. SECTORAL THREAT ANALYSIS

This section identifies and assesses ML threats to which the financial sector may be exposed. The criminal threats are determined based on reports submitted to the FIC. A breakdown of the number of FSCA regulated entities that were registered with the FIC as at 31 March 2018 and the different types of reports filed over the past two years is as follows:

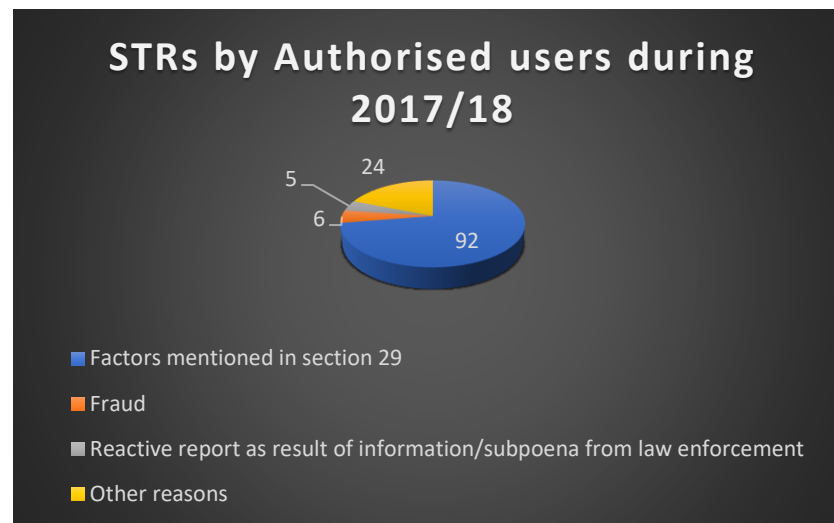
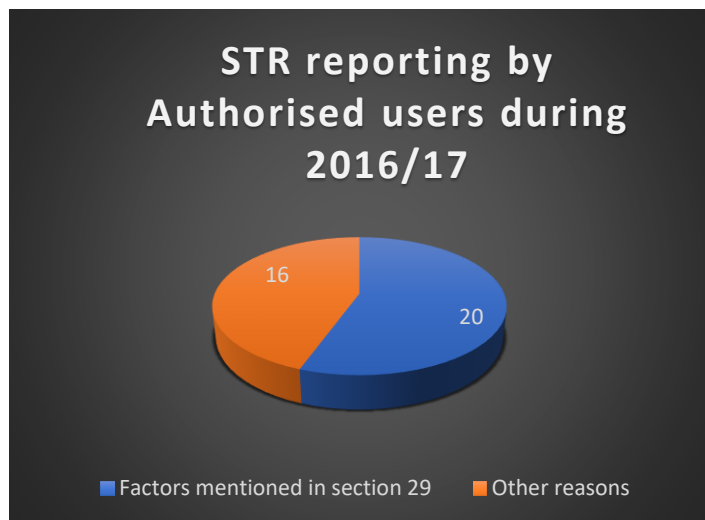
Sector	Registration with the FIC as at 31/03/2018	Number of STRs for the 2016/17-2017/18 financial years	Number of CTRs for the 2016/17-2017/18 financial years	Number of TPRs for the 2016/17-2017/18 financial years	Sec 27 requests for the 2016/17-2017/18 financial years
Authorised users	184	163	77 386	0	210
CIS	85	189	2 635	0	232
FSPs	8 556	3 574	43 285	0	11 249

The threats are based on the types of offences reported in the STRs. The number of STRs filed by the three sectors in the past two years is depicted below:

Period	Authorised users	CIS Managers	FSPs	Overall contribution
2016/17	36	125	2 410	0.72%
2017/18	127	64	1 164	0.41%

The above Table shows a general decrease in the number of STRs filed by CIS Managers and FSPs in recent years, while the securities sector saw an increase. The number of STRs filed by the three sectors for the period 2016/17 and 2017/18 is relatively low compared to other sectors as it represents 0,72% and 0,41% respectively of the total number of STRs filed by all accountable institutions.

Threats in the Securities Sector (Authorised users)

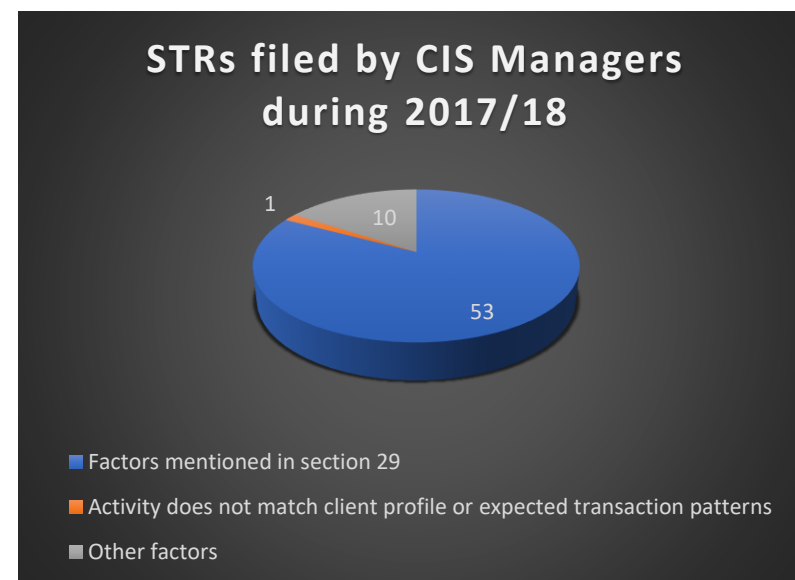
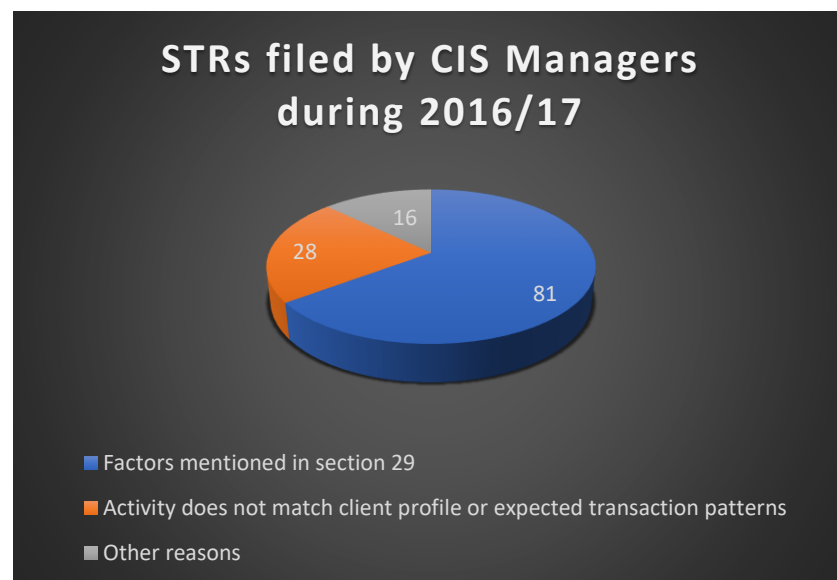


- As at 31 March 2018 a total of 184 Authorised users were registered with the FIC. About 53% of them filed STRs with the FIC. There has been a substantial increase in STRs from the 2016/17 financial year to the 2017/18 financial year (353% increase), yet it remains low compared to other sectors. The reason for submitting STRs related to suspicious and/or unusual transactions/activities mentioned in section 29 of the FIC Act, followed by fraud. Section 29 of the FIC Act directs AIs to report transactions if:
 - The business has received or is about to receive the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;
 - A transaction or series of transactions to which the business is a party –
 - Facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;

- Has no apparent business or lawful purpose;
 - Is conducted for the purpose of avoiding giving rise to a reporting duty under the FIC Act;
 - May be relevant to the investigation of an evasion or attempted evasion of a duty to pay tax, duty or levy imposed by legislation administered by the Commissioner of the South African Revenue Service;
 - Relates to an offence relating to the financing of terrorist and related activities; or
 - Relates to the contravention of a prohibition under section 26B; or
 - The business has been used or is about to be used in any way for money laundering purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities.
- A total of 77 386 CTRs were filed by Authorised users during the period under review. This amounts to 0,8% of the total number of CTRs filed. There seems to be limited cash usage in the securities sector. The CTRs filed by Authorised users are, however, substantially more than those filed by CIS managers (2 635) and financial services providers (43 285).
 - No reports were filed by Authorised users relating to terrorist financing transactions for the period under review.
 - The FIC issued 210 requests in terms of section 27 of the FIC Act to Authorised users to enquire if a specific person is or has been a client of the Authorised user. There were 51 (24,3%) positive responses.
 - The major concern for the sector, as per STRs filed, is where people claiming to be clients want to withdraw funds using fraudulent or falsified documentation. Another concern is insider trading which is the trading of securities by individuals with access to non-public information about the company.

As a result of the afore-mentioned, the securities sector is **low risk** from a threat analysis perspective.

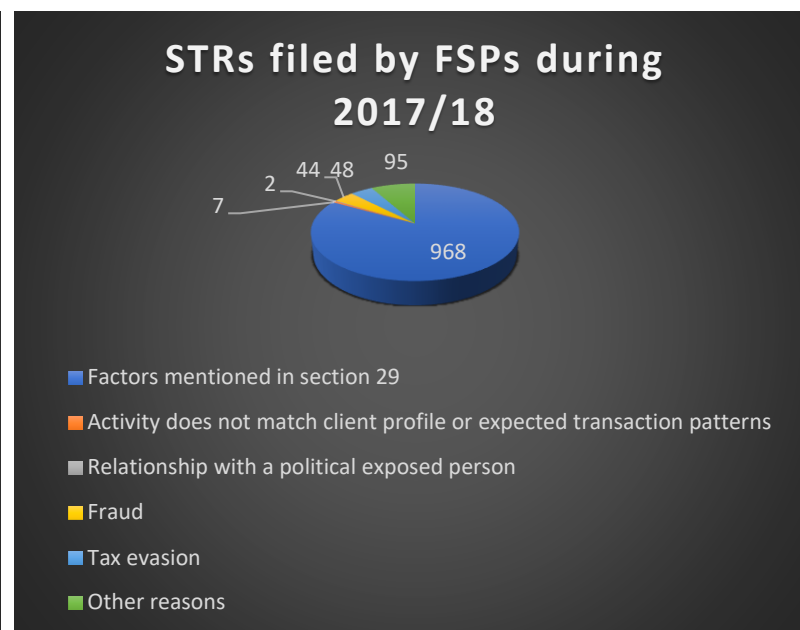
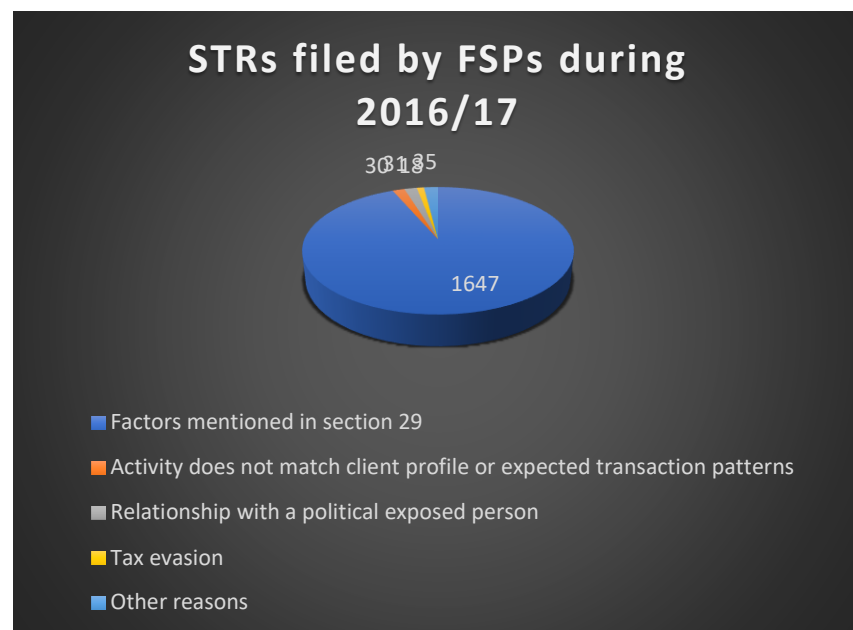
Threats in the CIS Sector (CIS Managers)



- As at 31 March 2018 a total of 85 CIS Managers were registered with the FIC. About 69% of them filed STRs during the period under review. There has been a substantial decrease in STRs between the 2016/17 and 2017/18 financial year. The reason provided for filing STRs related to suspicious and unusual transactions/activities as mentioned in section 29 of the FIC Act, followed by activities that do not match client profiles.
- A total of 2 635 CTRs were filed by CIS Managers during the period under review. This amounts to 0,03% of the total number of CTRs filed. There is therefore limited usage of cash in the CIS industry.
- No reports were filed by CIS Managers relating to terrorist financing transactions for the period under review.
- The FIC issued 232 requests in terms of section 27 of the FIC Act to CIS Managers to enquire if a specific person is or has been a client of the CIS Manager. There were 115 (50%) positive responses.
- There are no specific ML/TF concerns in this sector.

As a result of the afore-mentioned, the CIS sector is **low risk** from a threat analysis perspective.

Threats in Financial Services Sector (FSPs)



- As at 31 March 2018 a total of 8 556 FSPs were registered with the FIC. There were however 11 075 authorised FSPs licensed by the FSCA during this period. This means that a total of 22,7% of authorised FSPs were not registered with the FIC.
- There has been a substantial decrease in STRs during 2016/17 and 2017/18 financial years. About 26,7% of the authorised FSPs registered with the FIC filed STRs during the period under review. The reason provided for filing STRs related to suspicious or unusual transactions/activities as mentioned in section 29 of the FIC Act, followed by activities that do not match client profiles.
- A total of 43 285 CTRs were filed by FSPs during the period under review. This amounts to 0,5% of the total of CTRs filed. There is therefore limited usage of cash in the sector.
- No reports were filed by FSPs relating to terrorist financing transactions during the period under review.

- The FIC issued 11 249 requests in terms of section 27 of the FIC Act to FSPs to enquire if a specific person is or has been a client of the FSP. There were 1 630 (14,5%) positive responses.
- The major concern in this sector, as per STRs filed, relates to unlicensed businesses. Ponzi schemes are also a concern. The other issues are fraud and tax evasion.

As a result of the afore-mentioned, the financial services sector is **low risk** from a threat analysis perspective.

Taking into account all the sectors, the major common issues reported in STRs which point to possible ML threats are:

- Unauthorised business;
- Ponzi schemes;
- Fraud;
- Insider trading; and
- Tax evasion

Accordingly, the overall threat for the financial sector has been assessed and rated as follows:

Authorised users	CIS managers	FSPs			
		Financial advisers & Intermediaries	Investment managers	Hedge fund managers	LISPs
Low	Low	Low	Low	Low	Low

F. SECTOR VULNERABILITY ANALYSIS

The following section describes vulnerabilities of the different sectors regulated by the FSCA. A range of factors were considered in this assessment, including the nature of services offered by a sector and the compliance within that sector.

Vulnerabilities of the Securities sector (Authorised users)

Overview

The securities sector is regulated in terms of the Financial Markets Act, 2012. Participants in the securities sector (as at 31 March 2018) are Exchanges (5), CSDs (2), Nominees (FSCA: 72, JSE: 47, Strate: 26) and Authorised users (181).

Exchanges	Members/Authorised users	Equity listings	Market capitalisation
JSE	158	371	R14,2 billion
A2X	12	5	R44,7 million
4AX	1	4	R2,5 billion
ZAR	9	3	R3,2 billion
EESE	1	1	R423 million

Authorised users are authorised by a licensed exchange in order to perform one or more securities services in terms of the exchange rules. Authorised users can act as agents or as principal. Authorised users match orders of buyers and sellers without taking ownership of the securities. Authorised users may hold membership of more than one exchange. Trading is usually conducted on an “execution only” basis; but can be on “advised” or “managed account” basis. Authorised users can also offer custodian services.

ML Risk

The securities sector is one of the industries through which persons and entities can access the financial system. The securities sector in SA may be attractive for criminals to launder their illicit proceeds due to certain features such as use of cash, large values of

transactions, complex products, speed of execution of transactions and global reach through participation of foreign investors. Since cash does not seem to be used on a large scale in securities transactions, the sector is less conducive to the placement of illicit funds; but is more likely to be used in the layering and integration stages, where proceeds can be converted to assets such as securities.

According to the survey, 88% of the respondents have conducted an assessment in the business to understand ML risks to which they may be exposed.

Research on Money Laundering through the Securities Sector conducted by the ESAAMLG in 2015 assessed the securities sector in the region as low risk. However, the study found that there are indicators of ML/TF risks in the securities market which renders the sector vulnerable; but stated that these risks can be mitigated. The survey shows that the securities sector in SA is most vulnerable when compared to other sectors regulated by the FSCA and was assessed as **Medium**.

Vulnerabilities

The following are specific features of the Authorised users and their vulnerabilities to ML.

Risk Factors	Ratings	Results of the survey
Clients	High	Mostly individuals, but survey shows that 90% of the funds traded are for institutional clients.
High-risk clients		High prevalence of high-risk clients - Legal persons (91%), Trusts (69%), NGOs (33%), and NPOs (38%).
Foreign clients		High prevalence of foreign clients - foreign individuals (53%) and foreign institutions (56%)
Products	Medium	Low level of vulnerability to ML.
Anonymity		It is exceptionally difficult or impossible to mask a client's identity using securities (only 4%)
Cash		Used on a limited scale in this sector. Only 9% of the respondents accepted cash but have a reporting obligation to mitigate the risk.

Cooling-off period and refunds		Funds that have been deposited but not yet invested are available for immediate withdrawal. Securities can be sold in the market at any time.
Cross-border		Significant portion of the business involves cross-border transacting. The activity is carried out by banks through the national payment system.
Third party transacting		24% of respondents made payments to and received payments from third-parties other than the client
Distribution channels	Medium	Mostly online trading and minimal face-to-face interaction. About 62% of respondents relied on FSPs, group entities or third parties for clients and CDD.
Geographic location	Low	Limited dealings with clients from sanctioned countries, or from countries known to have excessive client confidentiality restrictions, or from countries having no or weak AML/CFT requirements (7%)
AML/CFT measures		Have processes, procedures and systems in place. No serious non-compliance observed
Overall vulnerability	Medium	

Taking into account the above features, the vulnerability levels for the securities sector is assessed as Medium.

Vulnerabilities of the CIS Sector (CIS Managers)

Overview

The CIS industry is regulated in terms of CISC. A CIS is an investment vehicle that allows investors to pool funds and invest in assets which they might not otherwise be able to access in their individual capacities. Investors are allocated a participatory interest or units, in proportion to the value of their contribution to the portfolio. Investors do not have control over assets purchased with their funds. Instead, they enjoy the benefits of a diversified portfolio managed by a registered CIS Manager, but in many cases this function is delegated to the Investment manager authorised under the FAIS Act through a delegation agreement.

The size of the CIS sector as at 31 March 2018 was as follows:

Type of Scheme	Number of CIS Managers	Assets under management
CIS in Securities	51	R2.17 trillion
CIS in Property	1	R0.96 billion
CIS in Participation Bonds	1	R2.07 billion
CIS in Hedge Funds	15	R89 billion

ML Risk

The CIS industry is likely to be used for layering illegitimate funds only. The risk of abuse for money laundering is increased by the fact that most transactions for new subscriptions, top-up investments, redemptions or switches are not conducted on a face-to-face basis. However, the risk is mitigated by the fact that most of these transactions involve authorised FSPs.

CIS Managers understand ML risks in their business. According to the survey, 90% of the respondents indicated that they have conducted an assessment across clients, products and services, distribution channels and geographic locations.

5.2.3 Vulnerabilities

The following are specific features of the CIS Managers and their vulnerabilities to ML/TF.

Risk Factors	Ratings	Results of the survey
Clients	Medium	Mixed clients consisting of individuals, corporates, institutional clients, both local and offshore
High-risk clients		High prevalence of high-risk clients - Legal persons (94%), Trusts (72%), NGOs (59%), NPOs (66%) and PEPs (53%)
Foreign clients		Large proportion of foreign clients - foreign individuals (78%) and foreign institutions (50%).
Products	Low	Less sophisticated. CIS in Hedge Funds can be a bit complex due to strategies employed and underlying products.
Anonymity		Cannot be used to mask the client's identity
Cash		Limited use of cash (1% only). Use of section 104 & 105 accounts to mitigate the risk.
Cooling-off period and refunds		Obligated to process a client's request to terminate investment and return client funds.
Cross-border		Facilitate cross-border transfer of funds (about 25%) through banking and national payment system.
Third party transacting		Low incidence of third-party transacting – Only 28% made payments to third-parties and 56% received deposits from third-parties.
Distribution channels	Medium	Both face-to-face and non-face-to-face transacting.
Geographic location	Low	Limited dealings with clients in sanctioned countries, those with excessive client confidentiality restrictions, or those with no AML/CFT requirements (9%).
AML/CFT measures		Have processes, procedures and systems in place. No serious non-compliance observed
Overall vulnerability	Low	

The CIS industry is assessed low risk from a vulnerability perspective.

Vulnerabilities of the Financial Services Sector (FSPs)

Overview

Financial services provider (FSP) is any person, other than a representative, who as a regular feature of the business of such a person, furnishes advice, renders an intermediary service, or provides both. FSPs are regulated under the FAIS Act.

The different types of FSPs authorised by the FSCA as at 31 March 2018 are as follows:

Number and Types of FSPs as at end of 2018	
Category I FSPs (Financial advisers & Intermediaries)	10 139
Category II FSPs (Investment managers)	670
Category IIA FSPs (Hedge fund managers)	127
Category III FSPs (Linked Investment Service Providers & Platforms)	28
Category IV FSPs	111

Vulnerabilities

Financial advisers & Intermediaries

Financial advisers & Intermediaries are considered a key segment of the financial services sector because they are the contact point between product suppliers and clients. Most Financial advisers & Intermediaries simply provide advice, do financial planning, sell products or help clients to select appropriate products for their financial needs. Most Financial advisers & Intermediaries do not handle client funds and are not allowed to make decisions on behalf of clients. There were 10 139 Financial advisers & Intermediaries authorised as Category I FSPs as at 31 March 2018.

ML Risk

Generally, most Financial advisers & Intermediaries do not hold client funds and are less likely to be involved in the placement stage of money laundering. However, they could still be abused in the layering and integration stages. Onsite and off-site inspections

conducted since 2014 revealed that most smaller Financial advisers & Intermediaries demonstrated low AML/CFT awareness levels and had inadequate controls. However, 96% of the respondents indicated in the survey that they have conducted an assessment to understand ML risks.

The following are specific features of the Financial advisers & Intermediaries and their vulnerabilities to ML.

Risk Factors	Ratings	Results of the survey
Clients	Medium	Mixed profile consisting of individuals and institutions, both locally and offshore. Individuals are in the majority.
High-risk clients		Large number of high-risk clients - Legal persons (61%), trusts (47%), NPOs (17%), and NGOs (12%), PEPs (9%).
Foreign clients		Most do not have foreign clients, but some of their local clients may have emigrated offshore.
Products	Low	Mostly insurance, health, retirement and investments. Most products are regulated by the FSCA and are issued by product suppliers that are also regulated.
Anonymity		Products sold cannot mask client's or beneficiary's identity.
Complexity		Less sophisticated in nature and are considered low risk for ML purposes.
Cash		Most do not handle client funds or accept cash in the business.
Cooling-off periods and refunds		Can cancel the contract upon request and refund monies where no benefit has yet been paid or claimed.
Cross-border		Very minimal. Carried out by the banking and national payment system.
Third party transacting		Very minimal, high prevalence of face-to-face transacting.
Distribution channels	Low	Most meet clients in person to establish long-lasting business relationships.
Geographic location	Low	Limited dealing (only 1%) with clients from sanctioned countries, or from countries with no AML/CFT requirements or countries with excessive client confidentiality requirements.
AML/CFT measures		Low level of awareness and inadequate control measures
Overall vulnerability	Low	

Financial advisers & Intermediaries have been assessed low risk from a vulnerability perspective.

Investment managers

Investment managers render an intermediary service in respect of a choice of financial products. They manage assets on behalf of clients in accordance with mandates signed with clients. As at 31 March 2018, there were 670 Investment managers operating in SA that are authorised as category II FSPs.

Investment managers can act with or without discretion.

- A discretionary Investment manager employs specialised skills and expertise to decide upon asset selection and to undertake transactions in a portfolio for the benefit of the client according to an investment mandate from the client.
- A non-discretionary Investment manager needs authority or consent from the client to make decisions on their behalf.

The Investment manager can perform the following activities:

- Manage the assets on a CIS portfolio on behalf of the CIS Manager in accordance with the founding mandate of the portfolio concerned, without interacting with the underlying investors.
- Manage a portfolio of assets for a specific investor (institutional, corporate or high net worth client), on a segregated basis, in accordance with a discretionary mandate agreed to with the client concerned.
- Manage one or more of the co-branded portfolios, on behalf of the CIS Manager, which are marketed and distributed by the Investment manager (often through financial advisers in its group or third-party distribution channels) to investors. In some cases, the Investment manager itself is also a financial adviser.
- Designs and constructs bespoke model portfolios for a group of clients or individual investors; in most cases by selecting existing CIS portfolios. These model portfolios can also be marketed and distributed to clients through their own Category I license, or by other financial advisers in the group or third-party distribution channels.
- Perform no or very little portfolio design, asset selection, or portfolio management. The Investment manager uses the discretionary mandate for the sake of convenience in order to obviate the need to obtain new written instructions from the client whenever portfolio switches are made between existing structures.

ML Risk

The industry exhibits certain features, such as large assets under management, complex products and services, personalised service and a culture of confidentiality, that makes it highly vulnerable to ML risk. The industry could be exploited at all three stages of the ML/TF model, i.e. placement, layering and integration.

A clear understanding of ML risks is important in order to combat ML risks. The survey revealed that 96% of the respondents have conducted an assessment in their businesses with a view to understand ML risks.

The following are specific features of Investment managers and their vulnerabilities to ML.

Risk Factors	Ratings	Results of the survey
Clients	High	Mostly individuals (high networth clients, professionals), corporates (trusts, close corporations, companies), and institutional clients (pension funds, insurers), both domestic and foreign.
High-risk clients		High interaction with high risk clients - Legal persons (78%), Trusts (70%), NGOs (9%), NPOs (21%) and PEPs (15%).
Foreign clients		Mainly local clients. Foreign individuals (31%) and foreign institutions (10%).
Products	Medium	Mainly equities, bonds, cash, ETFs and property.
Anonymity		Products invested in can mask a client's identity or allow beneficiaries to remain anonymous.
Complexity		Products invested in are complex. Use Nominee accounts to hold assets in safe custody.
Cash		Hardly involve cash, only 1% of respondents accepted cash, but have a reporting obligation.
Cooling-off periods and refunds		Must terminate the mandate upon written request and return client funds accordingly.
Cross-border		Frequently engages in cross-border transactions (48%). Facilitated by authorised users and banks through national payment system.
Third party transacting		Minimal. About 20% made payments to third parties and 11% received payments from third-parties.

Distribution channels	Medium	Mostly face-to-face contact and engagement with the client. Word of mouth for individuals and direct pitching to corporates and institutional clients
Geographic location	Low	Minimal investing (1% only) in sanctioned countries, or in countries with no AML/CFT requirements or countries with excessive client confidentiality requirements.
AML/CFT measures		Have processes, procedures and systems in place. No serious non-compliance observed
Overall vulnerability	Medium	

The overall vulnerability for Investment managers is assessed as medium.

Hedge funds managers

A Hedge fund manager manages or makes decisions about the investments held in a hedge fund scheme, or fund of hedge funds. There were 127 hedge fund managers authorised as Category IIA FSPs as at 31 March 2018. Most would be appointed by CIS Managers to manage their CIS Schemes in Hedge Funds.

Hedge funds have been declared as Collective Investment Schemes and are regulated in terms of Cisca. With the advent of regulation in 2015, most hedge fund managers, who are licensed as Category IIA FSPs, opted to place their funds on a CIS Manager's platform instead of procuring registration as CIS Managers for purposes of the hedge funds that they were managing.

ML Risk

Before the introduction of regulation in 2015, most hedge funds used the *en-commandite* structure to pool investors' funds but have since converted to the trust structure. As at 31 March 2018, there were only four CIS Schemes in Hedge Funds left that were still run on an *en-commandite* structure.

The *en-commandite* structure added a layer of opacity that could increase money laundering risk. The regulation now requires hedge funds to be more transparent and this significantly reduces the ML risk.

Most hedge fund managers understand the risk in their business. According to the survey, about 81% of the respondents indicated that they have done an assessment to identify and understand ML risks to which their business may be exposed.

The following are specific features of the Hedge fund managers and their vulnerabilities to ML.

Risk Factors	Ratings	Results of the survey
Clients	High	Qualified investors and institutional clients.
High-risk clients		Proportion of high-risk clients is high - Legal persons (73%), Trusts (47%), NGOs (7%), NPOs (13%) and PEPs (29%).

Foreign clients		Large proportion of foreign clients - foreign individuals (21%) and foreign institutions (47%).
Products	Low	Invest assets of a CIS Scheme in Hedge Funds in a wide range of products that are highly vulnerable as some of them could be unregulated.
Anonymity		Can invest in products that can mask a client's identity (6%). None invested in products that allow beneficiaries to remain anonymous
Complexity		En-commandite structure used to be highly complex. The trust structure currently utilised is more transparent and less sophisticated.
Cash		Do not invest in products that are cash intensive.
Cooling-off periods and refunds		Client can terminate investment in a CIS in hedge fund managed by a hedge fund manager any time.
Cross-border		Facilitate a significant amount of cross-border payments daily through an extensive correspondent banking system (50%).
Third party transacting		There are no third-party payments, however 20% received payments from third-parties.
Distribution channels	Medium	Can be face-to-face, but mostly place reliance on other parties.
Geographic location	Low	Not exposed to high risk jurisdictions. Do not invest in sanctioned countries, or countries with no AML/CFT requirements or with excessive client confidentiality requirements.
AML/CFT measures		Have processes, procedures and systems in place. No serious non-compliance observed
Overall vulnerability	Medium	

Hedge fund managers are assessed medium risk from a vulnerability perspective.

LISPs

A LISP is an independent company that offers access to a wide range of financial products that are placed on its platform through the method of bulking.

Bulking means –

- the aggregation of clients' funds when buying or investing in financial products on behalf of clients and the subsequent allocation of such financial products to each client separately.
- the aggregation of the financial products belonging to clients when selling such financial products on their behalf, and the subsequent allocation of the proceeds of such sale to each client separately.

A LISP usually functions in a non-discretionary capacity but may have discretionary mandates. A LISP does not own the products that it buys, sells or in which it invests. The investor owns them. A LISP merely holds, purchases or sells products on behalf of clients in bulked accounts. For protection, these products are held either in the name of the client or an independent custodian. A LISP must always reconcile buy and sell instructions received from clients with its records. There were 28 LISPs as at 31 March 2018.

ML Risk

A LISP is possibly vulnerable to money laundering risk in all stages i.e. placement, layering and integration stages of the cycle. The survey shows that 46% of the respondents have done an assessment to understand ML risks posed to the business.

Vulnerabilities

The following are specific features of the LISPs and their vulnerabilities to ML.

Risk Factors	Ratings	Results of the survey
Clients	High	Includes individuals, corporates (trusts, close corporations and companies), institutional clients (retirement funds), other FSPs and product suppliers (CIS Managers, insurers).
High-risk clients		High prevalence of high-risk clients - Legal persons (78%), Trusts (50%), NGOs (25%), NPOs (33%), PEPs (11%) and high net worth clients (50%).
Foreign clients		Interacts with foreign clients. Foreign individuals (56%) and foreign institutions (22%).
Products	Medium	Acts as one stop-shop and investment platform. Provides access to wide range of products such as CIS funds, ETFs, annuities and wrappers/portfolios.
Anonymity		Products cannot be used to mask the client's identity or allow beneficiaries to remain anonymous.
Complexity		Less sophisticated products and most of them are regulated.
Cash		Can receive cash for investment purposes, usually through deposits.
Cooling-off periods and refunds		Client can either personally or through a properly mandated FSP terminate its relationship with a LISP.
Cross-border		Can invest offshore by placing foreign products on the platform (about 22%). Cross-border transacting is done through banks and national payment system.
Third party transacting		About 22% made payments to third-parties and receive payments from third-parties on behalf of clients.
Distribution channels	Medium	Mostly non-face-to-face. Relies on other FSPs, group entities and third parties for CDD.
Geographic location	Low	Not exposed to high risk jurisdictions. Do not invest in sanctioned countries, or countries with no AML/CFT requirements or with excessive client confidentiality requirements.
AML/CFT measures		Have processes, procedures and systems in place. No serious non-compliance observed
Overall vulnerability	Medium	

The LISP sector is assessed Medium risk from a vulnerability perspective

Accordingly, in view of the various features described above, the financial sector has been assessed and rated as follows from a vulnerability perspective:

Authorised users	CIS managers	FSPs			
		Financial advisers & Intermediaries	Investment managers	Hedge fund managers	LISPs
Medium	Low	Low	Medium	Medium	Medium

G. CONSEQUENCES

Consequences refer to the impact or harm that ML/TF may cause and includes the effect of the underlying criminal and terrorist activity and, in this case, the financial sectors supervised by the FSCA.

Harm or loss to clients

Authorised users – Clients may lose confidence in the exchanges which will result in them not investing money in the sector. Clients may also suffer financial losses as a result of fraudulent activities on their accounts or insider trading.

CIS Managers – Clients may also lose confidence in this sector should it be abused by criminals. Clients may also not achieve the full investment benefits as a result of perceived criminal activities.

FSPs – Most FSPs do not deal with the client money directly and therefore the impact or harm would rather be reputational harm than financial harm.

Harm or loss to individual financial institutions

The controls put in place by the various sectors will minimise any harm or damage caused by ML/TF through these institutions. The controls largely refer to compliance with the FIC Act. Many Financial advisers & Intermediaries are not yet registered with the FIC. A natural deduction is therefore that they have no or limited AML/CFT controls in place. The sector also displays a low level of AML/CFT awareness and inadequate controls to manage potential ML/TF risks. The likelihood that Financial advisers & Intermediaries will be abused for ML/TF purposes are, however, low. This is, however, not the case with other types of FSPs in the sectors evaluated.

Other harm or loss consequences include:

- The financial institution may suffer financial losses as a result of being abused for criminal purposes;
- The financial institution may suffer reputational damage and as a result may lose clients;
- Other financial institutions may decide not to do business with the financial institution that was abused for ML purposes;
- Administrative sanctions being imposed by the FSCA on the financial institution or even debarments of individuals or revocation of the license;
- Criminal prosecution of persons in the financial institution for assisting another to benefit from proceeds of unlawful activities or to finance terrorist activities.

Harm or loss to the financial sector

The biggest harm to the sector is reputational damage. A bad reputation will inhibit the capital-raising process for listed companies and fewer investments will be made. Product suppliers may also decide not to make use of independent FSPs and only use 'in-house' agents.

Harm or loss to the South African economy

The following harm or loss to the South African economy will occur should ML/TF occur in the industries assessed:

- Economic distortion and instability;
- Undermine integrity of the financial system;
- Affect savings and investments; and
- Reduced revenue.

Accordingly, in view of the various features described above, the financial sector has been assessed and rated as follows from a consequence perspective:

Authorised users	CIS managers	FSPs			
		Financial advisers & Intermediaries	Investment managers	Hedge fund managers	LISPs
Medium	Medium	Low	Medium	Medium	Medium