SOUTH AFRICAN RESERVE BANK
Prudential Authority

PRUDENTIAL AUTHORITY

Assessment of money laundering, terrorist financing and proliferation financing risk in the banking sector

July 2022

Contents

1. Executive summary

The Prudential Authority (PA) of the South African Reserve Bank (SARB) is responsible for anti-money laundering and counter-financing of terrorism (AML/CFT) supervision of banks, mutual banks and life insurers. As such, the PA assesses the risks related to these aspects. It embarked on its second banking sector risk assessment by surveying 34 banks in March 2021. The 34 banks consisted of 4 subsectors, namely 5 large banks, 9 medium to small locally controlled banks, 17 foreign controlled banks and branches of foreign banks, and 3 mutual banks. The PA also engaged with various stakeholders, including central banks, the Financial Intelligence Centre (FIC) and law enforcement agencies, conducted independent research and consulted the Financial Surveillance Department of the SARB to obtain relevant information. This assessment focused on the money laundering, terrorist financing and proliferation financing (ML/TF/PF) risks identified within the banking sector for the period 1 October 2018 to 31 December 2020. For this report, the banking sector has been divided into four categories: large banks, medium to small locally controlled banks,[1] branches of foreign banks and foreign controlled banks, and mutual banks.

1.1 Threats and vulnerabilities

The common threats identified across the banking sector were:

- fraud, bribery and corruption;
- illegal investment scams (Ponzi/pyramid);
- environmental crimes;
- tax-related offences or crimes;
- illicit cross-border flows;
- criminals using money mules;

[1] These are the local banks, excluding mutual banks, that are not part of the five big banks in South Africa.

- drug trafficking and human trafficking; and
- cybercrime, including emerging technologies that may be used to commit crimes.

The common vulnerabilities identified across the banking sector were:

- an inability to identify domestic prominent influential persons (DPIPs);
- the inability of banks to obtain beneficial ownership information;
- the misuse of trade products and related services such as advanced payments;
- the identification of cryptocurrencies and exchanges (as client types);
- non-face-to-face client onboarding and interactions;
- products that allow large volumes of cash deposits;
- the lack of a single client view across a bank when a client has multiple business relationships or accounts with different business units within the same bank; and
- data issues, including misalignment, inaccuracies in and integrity of data.

1.2 Consequences

The consequences of ML and TF may be of a short- or long-term duration and relate to the business environment, nationally or internationally. The most significant consequence is financial loss as a result of financial crime and scam-related offences, and reputational damage for banks. In addition, bribery, fraud, corruption, cybercrime, tax evasion, illegal investment schemes and other related crimes may have a detrimental effect on the integrity of the banking sector and the South African economy as a whole.

Corruption affects the banking sector as banks may inadvertently process the bank accounts of government and salaried employees that are credited outside of the normal expected salary scope and may involve the proceeds of crime. This includes the potential abuse of state funds by politically exposed persons (PEPs), identified as foreign prominent public officials (FPPOs) and DPIPs in South Africa.

1.3 Money laundering, terrorist financing and proliferation financing

The nature and extent of ML/TF/PF threats the banking sector in South Africa is facing is assessed to be a **high risk.**

High			
Medium			
Low			
Scale	**Money laundering**	**Terrorist financing**	**Proliferation financing**

1.4 Predicate offences

The common predicate offences often identified through the reporting process for all 34 banks included:

- corruption;
- bribery;
- tax evasion;
- fraud;
- internet and related scams;
- drug trafficking;
- cryptocurrency related transactions; and
- illegal wildlife trade and pyramid schemes.

1.5 Overall risk rating

The banking sector risk assessment focused mainly on the inherent risk. The overall inherent ML/TF risk within the banking sector in South Africa is assessed to be **high**. Table 1 below summarises the assessed inherent ML/TF risk for each subsector.

Table 1: Overall banking sector inherent risk

Large banks	Medium to small locally controlled banks	Branches of foreign banks and foreign controlled banks	Mutual banks
High	Medium	High	Low

Large banks

These banks were assessed to have a **high** overall ML/TF risk in the South African banking sector. The five large banks hold 89% of the total assets for the banking sector, so their materiality to the sector is significant. They offer a wide range of complex, high-volume products and services and rapid speed of transactions. The products and services are offered to clients domestically and internationally. The large banks are exposed to all high-risk client types. One of the large banks indicated a total of 8 388 clients with unknown citizenship, which poses a high risk within the sector. A large bank indicated a total of 1 782 clients with the country of incorporation unknown. The subsector is still targeted by criminals as clients use cash extensively and can use non-face-to-face methods such as automated teller machines (ATMs) to deposit cash, while the source of funds and details of depositors are largely unknown.

The large banks submit 95% of their cash threshold reports (CTRs) to the FIC. This subsector processes cross-border transactions for a wider range of clients and for clients with more complex structures than in other subsectors. All large banks provide correspondent banking relationships (CBRs) with one large bank accounting for over 40% of vostro (an account a correspondent bank holds on behalf of another bank) and nostro (an account that a bank holds in a foreign currency in another bank) accounts in the subsector. Two of the five large banks held CBRs with nested accounts and one large bank had relationships with payable-through accounts. The large banks have a high exposure to foreign country risk, with large banks facilitating trillions of rands in international fund transfers. The large banks are also exposed to high-net-worth individuals and FPPOs.

The PA's analysis of the beneficial ownership information revealed that two of the five largest banks have the highest number of beneficial owners that were identified

as DPIPs, and one of the five large banks also had the highest number of beneficial owners identified as FPPOs across the sector. The large banks are faced with clients with complex company structures, and this could be used to obscure the true beneficial ownership of funds. One large bank had banked the highest number of non-profit organisations (NPOs) across the banking sector. One large bank had banked over 90% of foreign trusts where the AML/CFT risk ratings were unknown. These areas were identified as posing vulnerability to the banking sector due to the high risk associated with obtaining the client due diligence (CDD) information for DPIPs, FPPOs and beneficial owners as well as the lack of obligatory registrations for the NPOs.

In summary, large banks are widely exposed to a high level of inherent ML/TF risk. This is as a result of their high numbers of clients, substantial exposure to foreign country risk, use of non-face-to-face delivery channels which increases anonymity, very high exposure to cash, and the propensity for the illicit flow of funds.

Medium to small locally controlled banks

The ML/TF risk associated with the locally controlled banks (other than the five largest banks) was assessed to be **medium** due to their large client base, significant exposure to cash and increasing use of remote service delivery channels.

There are various factors that expose the subsector to high ML/TF risks. The subsector has a large client base, second to the large banks, and is exposed to high-risk client types. The subsector includes as clients several foreign natural persons, trusts, NPOs and legal persons with complex structures. The subsector also offers financial inclusion products to clients with limited CDD information, such as the lack of a registered address.

Although the locally controlled banks contribute an insignificant percentage of 3.28% to the overall CTR submissions to the FIC, this subsector is exposed to cash which increases its ML/TF vulnerability. The digital banks indicated the movement of cash by their clients as one of the ML/TF vulnerabilities.

Increased remote service delivery channels, such as the use of ATMs and online banking, can facilitate identity fraud, contribute to the anonymity of persons and make it difficult to detect suspicious and unusual transactions. Two of the locally controlled banks offer contactless or digital banking services, where the anonymity of clients and the rapid movement of transactions increased ML/TF risk. Only two banks offer CBRs. In addition, the locally controlled banks are exposed to foreign country risk, as they participate in international funds transfers. These banks also offer trade finance products and services, an area which is traditionally regarded as a high risk for ML/TF activities.

Although the subsector was assessed to be of medium risk overall, some banks within this subsector pose a higher ML/TF risk to the banking sector. Those banks have other higher-risk factors, such as beneficial owners linked to DPIPs and to foreign entities, mule accounts, products that allow for large volumes of cash, and a vulnerability to ML activities.

Branches of foreign banks and foreign controlled banks

The overall ML/TF risk rating of the branches of foreign banks (hereafter referred to as foreign branches) was assessed to be **high** due to the significant exposure to foreign country risk. Although these branches, for the most part, bank fewer clients and offer fewer to no retail banking services than some local banks, they are exposed to a small number of high-risk clients that conduct cross-border transactions and offer complex high-risk products. These products include trade finance, the use of CBRs, agent bank arrangements, and investment products and services that may hide the source and destination of illicit funds. Certain foreign branches have a high exposure to FPPOs, and beneficial owners linked to foreign entities. One foreign branch had a significant number of FPPOs in relation to the total subsector.

This subsector has a high share of high-risk clients. These include trusts, high-net-worth clients, financial institutions and foreign-based clients. The foreign branches are exposed to mostly legal person client types; however, two banks had more than

50% of total foreign natural persons. The subsector also conducts business in high-risk jurisdictions due to its clients and products and services offered.

Mutual banks

The ML/TF overall inherent risk for mutual banks was assessed to be **low**. This category accounts for a smaller percentage of the overall banking sector in terms of asset size and clients, and typically offer retail products and services to South African low- and middle-income earners. Their client base predominantly comprises of individuals that take up simple product offerings. A vulnerability identified in mutual banks is that most of their clients were onboarded digitally. Mutual banks have limited to no exposure to foreign country risk as they operate primarily in South Africa and do not offer banking services to corporate clients – instead they only offer services to small- and medium-sized South African businesses.

2. Introduction

The second ML/TF/PF banking sector risk assessment was compiled by the PA to understand the level of these risks in South Africa. The assessment reflects the ML/TF/PF risks identified within the sector for the period 1 October 2018 to 31 December 2020. The PA distributed a risk assessment survey to 34 banks.[2] It consisted of questions pertaining to a bank's understanding of the ML/TF/PF risks.

[2] Banks: Absa Bank Limited, FirstRand Bank Limited, Investec Bank Limited, Nedbank Limited, Standard Bank South Africa Limited, African Bank Limited, Bidvest Bank Limited, Capitec Bank Limited, Discovery Bank Limited, Grindrod Bank Limited, Ithala SOC Limited, Sasfin Bank Limited, TymeBank Limited, Ubank Limited, Access Bank South Africa Limited, Al Baraka Bank Ltd, Bank of China Limited (Johannesburg branch), Bank of Communications Co. Ltd (Johannesburg branch), Bank of Taiwan (South Africa branch), BNP Paribas (South Africa branch), China Construction Bank Corporation (Johannesburg branch), Citibank NA, Deutsche Bank AG, Goldman Sachs International Bank (Johannesburg branch), Habib Overseas Bank Limited, HBZ Bank Limited, HSBC Bank Plc (Johannesburg branch), ICICI Bank Limited, JPMorgan Chase Bank (Johannesburg branch) , Standard Chartered Bank, State Bank of India, Bank Zero Mutual Bank, Finbond Mutual Bank and GBS Mutual Bank.

3. Purpose of the banking sector risk assessment

The purpose of the banking sector risk assessment is to identify the ML/TF/PF risks in the sector, and to assist the PA in developing a collective view of these risks in order to assist in further appreciating the ML/TF/PF risks across the banking sector to aid its supervisory activities as appropriate. Furthermore, this assessment provides policymakers with more insight into the outcomes of the current AML/CFT regime in South Africa. The emphasis of the assessment was on inherent risk[3].

4. The AML/CFT framework of the Prudential Authority

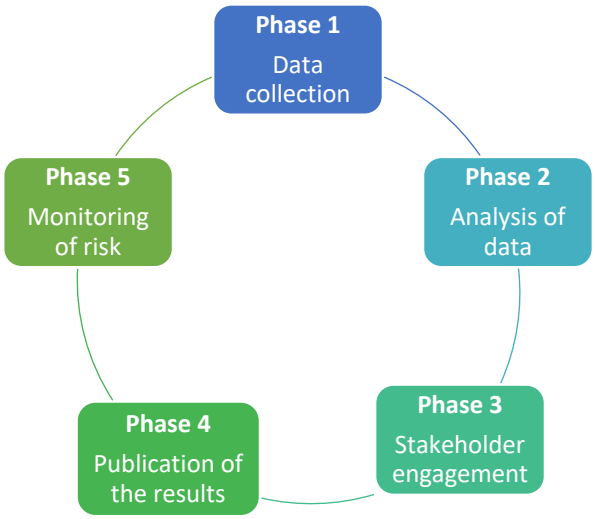
The PA is responsible for AML/CFT supervision of inter alia banks and mutual banks. The PA must ensure that these said accountable institutions (AIs) comply with the requirements of the Financial Intelligence Centre Act 38 of 2001, as amended (FIC Act). Schedule 2 of the FIC Act designates the PA as a supervisory body in respect of inter alia the banks and mutual banks.

5. Approach in conducting the banking sector risk assessment

The PA engaged various stakeholders, including law enforcement agencies and other central banks or agencies, to obtain data that could help provide an independent view of the risks in the banking sector, in addition to the data obtained from the banks. The results of the assessment include qualitative and quantitative data that was considered.

[3] Inherent risk is the risk of an event or circumstance that exists before controls or mitigation measures are applied by the accountable institution

Figure 1: Five-phase approach to the banking sector risk assessment



6. Methodology

The methodology applied follows the guidance of the Financial Action Task Force (FATF), which states that ML/TF risks can be seen as a function of criminal threats, vulnerabilities and consequences. In this assessment:

Threat is a person or a group of people, an object or an activity which has the potential to cause harm to the bank. The threats were determined by analysing the information obtained from the banks to understand the likelihood of these risks occurring and the impact that they would have on the banking sector.

Vulnerability refers to the things that can be exploited by a threat or may support or facilitate harmful activities. These vulnerabilities leave the banking sector open to abuse by criminals wishing to launder money and finance terrorism and proliferation.

Consequences refer to the impact or harm that ML/TF activities may cause and include the effects of the underlying criminal or terrorist activity on financial systems and institutions.

The assessment considered eight inherent risk factors and various key or sub-risk indicators per factor. The sub-risk factors consisted of a comprehensive list of risk factors. Each risk factor and sub-risk factor was assigned a weighting, and an average risk score was determined for each of the four banking categories. Each category was weighted, and an average risk score determined the overall inherent

risk rating for the subsector. Each subsector was then assigned a percentage weight based on its materiality and risk to the banking sector.

The subsector percentage weight was assigned as 70% for large banks, 10% for locally controlled banks, 15% for branches of foreign banks and 5% for mutual banks. The overall inherent risk rating score and the percentage weight per the subsector was used to calculate the overall banking sector risk rating. Table 2 depicts the inherent risk factors and the risk weightings allocated.

Table 2: Inherent risk factors

Inherent risk factors	Risk weighting
Asset size	10%
Client risk	30%
Product risk	15%
Delivery channel	10%
Geographical risk	9%
Terrorism financing risk	8%
Proliferation financing risk	8%
Other risk factors	10%
Total risk weight	**100%**

Table 3 depicts the risk categorisation, risk rating score and risk weighting.

Table 3: Risk scale and weighting

Risk rating category	Risk rating score	Weighting
Low risk	0–1 point	0–1.4
Medium risk	2 points	1.5–2.4
High risk	3 points	2.5–3

The risk rating considered numerous factors, taking into account the listed inherent risk factors, the sub-risk factors, adverse media coverage, outcomes of the PA's supervision expertise and data from other sources.

Table 4: Inherent risk factors and risk weighting per subsector

Inherent risk factors and description	Large banks	Medium to small locally controlled banks	Branches of foreign banks and foreign controlled banks	Mutual banks
Asset size	0.3	0.2	0.2	0.1
Client risk	0.9	0.75	0.77	0.38
Product risk	0.465	0.38	0.365	0.175
Delivery channel	0.275	0.2825	0.2125	0.12
Geographical risk	0.25	0.14	0.27	0.09
Terrorism financing risk	0.2	0.22	0.2	0.14
Proliferation financing risk	0.2625	0.2325	0.2425	0.1425
Other risk factors	0.3	0.24	0.24	0.15
Total risk weight	**2.9525**	**2.445**	**2.5**	**1.2975**
Risk category per subsector of banks	**High**	**Medium**	**High**	**Low**

The following information sources were also considered for this report and to determine the overall banking sector risk rating:

- data received from the banking sector through the surveys and risk return submissions;
- analysis of the regulatory reports filed with the FIC by the banking sector for the period 1 October 2018 to 31 December 2020;
- AML/CFT inspection reports for the period 1 October 2019 to September 2020;
- open source information, including public information produced by governmental agencies, other private institutions and the media;
- consultation with other stakeholders, such as law enforcement agencies and other central banks;
- independent research via publicly available information;
- published national risk assessments and sectoral risk assessments;
- data on ML/TF/PF risks, threats and vulnerabilities; controls to mitigate and manage these; countries with the highest volume of electronic transfers to and

from South Africa; and statistics pertaining to the attachment or confiscation of cross-border movement of funds received from Authorised Dealers; and

- information received from the SARB's Financial Surveillance Department on the inward and outward flow of funds, transaction categories, ML schemes and movement of illicit funds practices.

Annexure A provides details pertaining to the methodology applied for the banking sector risk assessment and Annexure B provides details of the overall banking sector risk rating calculation.

7. The nature and size of the banking sector

In South Africa, there are currently 34 licensed deposit-taking entities. These entities comprise 5 large banks, 9 medium to small locally controlled banks (hereafter referred to as locally controlled banks)[4], 17 branches of foreign banks and foreign controlled banks (hereafter referred to as foreign banks), and 3 mutual banks (collectively referred to as financial institutions or banks). Of these 34 financial institutions, the banking sector is dominated by five large banks, which collectively held 89.5% of the total banking sector assets as at 30 September 2021. At the same time, locally controlled banks held 3.9% of banking sector assets, branches of foreign banks and foreign controlled banks accounted for 6.5% of the assets, and the mutual banks accounted for 0.05% of the assets. Table 5 shows the total assets and number of clients for the banks as at 30 September 2021:

[4] These are the local banks that do not form part of the five big banks in South Africa, excluding mutual banks.

Table 5: Assets of the banking sector as at 30 September 2021

Categories of banks	Total assets of banks (R'000)	Percentage of assets	Number of clients	Percentage of clients
Large banks	R5 918 653	89.5%	35 913 593	57%
Locally controlled banks	R258 992	3.9%	26 400 499	42%
Branches of foreign banks and foreign controlled banks	R432 908	6.5%	274 319	0.44%
Mutual banks	R3 270	0.05%	164 835	0.26%
Total assets	**R6 613 823**	**100%**	**62 753 246**	**100%**

The large banks offer a wide variety of services in comparison to other categories of banks, and the products and services generally comprise retail banking; corporate and investment banking; trade financing; home and motor vehicle financing; wealth and investment services; and business and commercial banking services.

8. Inherent risk assessment: clients

This section focuses on the assessment of the qualitative responses and quantitative data collected from the banking sector regarding inherent ML/TF risks. The assessment aims to provide a general view of the inherent ML/TF risks in respect of client types that presented a higher risk within the banking subsectors and the sector, with a focus on:

1. clients posing a higher degree of ML/TF risk, including:
    a. high-risk rated clients;
    b. clients domiciled in high-risk jurisdictions[5];
    c. clients onboarded using digital channels rather than face-to-face;
    d. corporate clients with complex and multi-layered structures;

[5] This is according to the banks' risk assessments conducted.

e. clients whose activities involve transacting in large amounts of cash;
f. clients whose activities involve cross-border movements of funds; and
g. clients in high-risk industries.

2. DPIPs;
3. FPPOs;
4. CBRs; and
5. NPOs.

8.1 Clients posing a higher degree of ML/TF risk

8.1.1 High-risk rated clients

Clients that presented an increased inherent ML/TF risk to the banking sector included clients that were risk rated as 'very high'; local and foreign clients; natural and legal persons; and new and existing clients. Some of the high-risk clients also included DPIPs and FPPOs.

Four banks banked the most high-risk clients, of which three were large banks and one was a smaller locally controlled South African bank. About 60% of all high-risk clients were located within the locally controlled banks and about 40% within the large banks. Table 6 provides a high-level overview of the high-risk client population per subsector.

Table 6: Overview of the high-risk clients

Categories of banks	Total high-risk clients	Percentage of total	Average number of high-risk clients	Highest number of high-risk clients
Large banks	161 960	39.408%	24 786	120 909
Medium to small locally controlled banks	248 253	60.405%	43 896	159 847
Branches of foreign banks and foreign controlled banks	652	0.159%	63	211
Mutual banks	119	0.029%	40	93
Total	**410 984**	**100%**		

8.1.2 Clients domiciled in high-risk jurisdictions

Table 7 outlines the high-risk jurisdictions where most of the banking sector's clients were domiciled according to the banks' risk assessments.

Table 7: High-risk jurisdictions ranked

Rank	Country	Jurisdiction with strategic deficiencies (FATF grey list)[6]
1	Zimbabwe	Yes
2	Mozambique	No
3	Mauritius	Yes
4	Nigeria	No
5	Democratic Republic of Congo	No
6	Kenya	No
7	Uganda	Yes
8	Pakistan	Yes
9	Botswana	Yes

Table 8 outlines the number of clients domiciled in high-risk jurisdictions according to the banks' risk assessments.

Table 8: Clients domiciled in high-risk jurisdictions

Categories of banks	Number of clients domiciled in high-risk jurisdictions	Percentage
Large banks	29 156	19.999%
Medium to small locally controlled banks	116 011	79.576%
Branches of foreign banks and foreign controlled banks	609	0.418%
Mutual banks	11	0.008%
Total	**145 787**	**100%**

[6] Jurisdictions under increased monitoring are actively working with the FATF to address strategic deficiencies in their regimes to counter ML/TF/PF. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the 'grey list'. Documents – FATF (fatf-gafi.org)

Most clients domiciled in high-risk jurisdictions were banked by one of the locally controlled banks. This was followed by one of the large banks (10.7%) and the four remaining large banks (aggregated at 9.3%). Two of the three mutual banks indicated that they did not bank clients domiciled in high-risk jurisdictions. Two foreign branches banked almost all the clients domiciled in high-risk jurisdictions within that subsector.

8.1.3 Clients onboarded through digital channels

Table 9: Clients onboarded through digital channels[7]

Categories of banks	Number of clients onboarded through digital channels	Percentage of clients onboarded through digital channels
Large banks	1 721 350	77.514%
Medium to small locally controlled banks	496 296	22.349%
Branches of foreign banks and foreign controlled banks	717	0.032%
Mutual banks	2 319	0.104%
Total	**2 220 682**	**100%**

Most clients onboarded through digital channels (77.5%) were banked by the large banks. This was followed by locally controlled banks (22.3%) and foreign branches (0.03%). Only one of the three mutual banks onboarded clients digitally.

[7] Three banks indicated that all their clients were onboarded through digital channels; however they did not provide data.

8.1.4 Corporate clients with complex and multi-layered structures

Table 10: Total number of corporate clients (complex or layered)[8]

Categories of banks	Number of corporate clients that are part of complex or multi-layered structures of ownership or control	Percentage of corporate clients that are part of complex or multi-layered structures of ownership or control
Large banks	50 840	96.609%
Medium to small locally controlled banks	596	1.133%
Branches of foreign banks and foreign controlled banks	1 188	1.822%
Mutual banks	0	0%
Total	**52 624**	**100%**

Most corporate clients with complex or multi-layered structures were banked by large banks, as follows:

- bank one banked 50.3%;
- bank two banked 25.2%;
- bank three banked 18.2%; and
- bank four banked 2.8% of these clients.

This was followed by 1.8% of clients in the foreign branch subsector of which 80.7% were banked by one foreign branch, and another 12.1% and 4.7% of clients were banked by two more branches within the subsector. The remaining share of clients were banked by locally controlled banks. No mutual banks banked corporate clients with complex or multi-layered structures.

[8] One large, one small and one foreign controlled bank indicated that they did not have this information available and could therefore not provide the relevant data.

8.1.5 Clients involved in large cash transactions

Table 11: Total number of clients involved in transactions of large cash amounts[9]

Categories of banks	Number of clients involved in transactions of large cash amounts	Percentage of clients involved in transactions of large cash amounts
Large banks	441 498	95.274%
Medium to small locally controlled banks	21 848	4.715%
Branches of foreign banks and foreign controlled banks	52	0.011%
Mutual banks	0	0%
Total	**463 398**	**100%**

Table 11 indicates that most clients whose activities involve transacting in large amounts of cash were banked by large banks, as follows:

- bank one banked 63.6%;
- bank two banked 22.4%; and
- bank three banked 12.4% of these clients.

This was followed by 4.7% of clients banked in the locally controlled banks subsector, of which 81.3% were banked by one locally controlled bank. Two other locally controlled banks banked 15.4% and 2.5% of clients within the subsector. The foreign branches only banked 0.01% of clients. No mutual banks banked these clients.

Some banks indicated that they did not deal with cash, and sometimes cash was used in isolated instances. Additionally, there were banks that indicated that they

[9] One large bank and one locally controlled bank indicated that this data was not available.

did not have clients who transacted in large amounts of cash due to internal cash withdrawal restrictions.

8.1.6 Clients whose activities involved cross-border movements of funds

Table 12: Total number of clients involved in cross-border movement of funds[10]

Categories of banks	Number of clients involved in cross-border movement of funds	Percentage of clients involved in cross-border movement of funds
Large banks	2 069 327	95.619%
Medium to small locally controlled banks	89 191	4.121%
Branches of foreign banks and foreign controlled banks	5 620	0.259%
Mutual banks	0	0%
Total	**2 164 138**	**100%**

Table 12 indicates that most clients whose activities involved cross-border movement of funds were banked by large banks, as follows:

- bank one banked 41.4%;
- bank two banked 40.7%;
- bank three banked 11.0%; and
- bank four banked 2.5% of these clients.

This was followed by 4.1% of clients in the locally controlled banks subsector, of which 91.8% were banked by one bank. Two other locally controlled banks banked the remaining 3.5% and 3.1% of these clients. Foreign branches banked 0.3% of these clients, with one foreign branch banking 71.2% of these clients in the subsector. No mutual banks banked clients involved in cross-border movement of funds.

[10] Two of the large banks and one foreign bank confirmed that data was not readily available.

8.1.7 Client types identified as being more vulnerable to ML and TF

The following client types were identified as being more vulnerable to ML and TF risks:

- corporates or complex structures;
- treasury outsource, collective investment schemes, special purpose vehicles and private investment vehicles;
- government or state-owned entities;
- trusts;
- merchant services;
- partnerships;
- NPOs;
- stokvels;
- foreign individuals from high-risk jurisdictions;
- cash-intensive clients;
- clients involved in trade finance;
- CBRs with banks in third-world countries;
- wealth or private clients – privacy and complex products;
- transactions between high-net-worth clients; and
- clients operating in the following industries:
  - mining;
  - gambling;
  - defence; and
  - real estate.

8.1.8 Domestic prominent influential persons (including family members and known close associates)

The vast majority of DPIPs (83.7%) were banked by the large banks. This was followed by four locally controlled banks (15.2%), with the remaining locally controlled banks banking 0.3% of all DPIPs. Only 1.1% of all DPIPs were banked by foreign branches of which one foreign branch banked 40.7% of all DPIPs in this subsector. Mutual banks banked 0.07% of all DPIPs.

Table 13: Overview of DPIPs

Categories of banks	Number of DPIPs, associated parties and close family members	Number of DPIPs with adverse media	Number of DPIPs, associated parties and close family members rated as high-risk clients[11]
Large banks	22 605	2 916	9 231
Medium to small locally controlled banks	4 112	168	2 710
Branches of foreign banks and foreign controlled banks	288	22	142
Mutual banks	18	0	10
Total	**27 023**	**3 106**	**12 093**

Table 13 shows the percentage of total DPIPs with adverse media by subsector. These DPIPs were mostly banked by large banks (93.9% of DPIPs with adverse media) and locally controlled banks (5.4% of DPIPs with adverse media). One large bank banked 65.8% of DPIPs with adverse media, followed by two other large banks at 19.1% and 8.9%, respectively. Foreign branches only banked 0.7% of DPIPs with adverse media. No DPIPs with adverse media were banked by mutual banks.

In addition, Table 13 shows the percentage of total DPIPs which were rated as high risk by subsector. Almost half of all DPIPs were rated as high risk. Large banks' risk accounted for most of these DPIPs, followed by locally controlled banks. Foreign branches only banked 1.2% of all high-risk DPIPs, with one foreign branch banking

[11] One large bank indicated that this data was not readily available.

68.3% of these high-risk DPIPs. Mutual banks only banked 0.08% of all high-risk DPIPs.

8.1.9 Foreign prominent public officials

Table 14: Overview of FPPOs

Categories of banks	Number of foreign prominent public officials (FPPOs)	
Large banks	2 490	
Medium to small locally controlled banks	1 708	
Branches of foreign banks and foreign controlled banks	283	
Mutual banks	0	
Total	**4 481**	

The majority of FPPOs (55.6% of all FPPOs in the sector) were banked by large banks, followed by locally controlled banks (38.1%) and foreign branches (6.3%). No FPPOs were banked by mutual banks.

8.1.10 Correspondent banking relationships

Table 15: Overview of correspondent banking relationships

Categories of banks	Number of correspondent banking relationships (CBRs)	Number of CBRs rated as high risk	Percentage of high risk rated CBRS as percentage of total number of CBRs
Large banks	2 364	664	28.088%
Medium to small locally controlled banks	23	0	0%
Branches of foreign banks and foreign controlled banks	175	65	37.143%
Mutual banks	0	0	0%
Total	**2 562**	**729**	**28.454%**

Large banks accounted for 92.2% of all CBRs and 91% of all high-risk CBRs. In addition, 90% of high-risk CBRs were banked by three large banks. Foreign branches accounted for 6.8% of all CBRs and 8.9% of high-risk CBRs. Two foreign branches banked 80% of these high-risk CBRs within the subsector. Locally controlled banks and mutual banks did not have any high-risk CBRs.

Figure 2: Vostro[12] and nostro[13] accounts

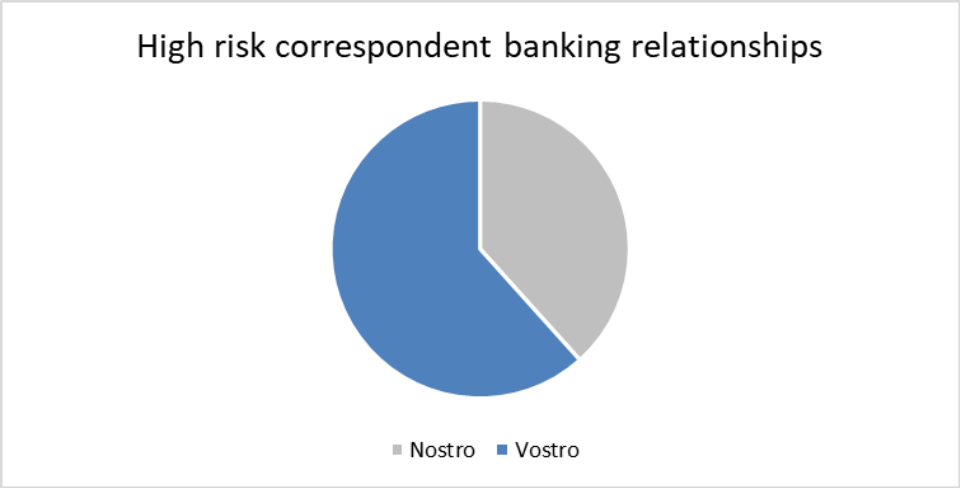


Table 16: High-risk vostro CBRs

Total CBRs	Total high-risk CBRs	High-risk vostro CBRs	High-risk vostro CBRs as a percentage of total CBRs	High-risk vostro CBRs as a percentage of total high-risk CBRs
2 556	730	454	17.762%	62.192%

Table 17: High-risk nostro CBRs

Total CBRs	Total high-risk CBRs	High-risk nostro CBRs	High-risk nostro CBRs as a percentage of total CBRs	High-risk nostro CBRs as a percentage of total high-risk CBRs
2 556	730	280	10.955%	38.357%

[12] A vostro account is an account a correspondent bank holds on behalf of another bank.
[13] A nostro account refers to an account that a bank holds in a foreign currency in another bank.

About 28.6% of all CBRs were rated as high-risk, of which 62% were vostro and 38% were nostro. In addition, 70% of all high-risk nostro accounts and 91% of all high-risk vostro accounts were banked by the large banks.

8.1.11 Non-profit organisations

8.1.11.1 Types of non-profit organisations

The following table outlines the various types of NPOs and their respective risk ratings, as indicated by the participating banks. Nine banks indicated that they did not bank NPOs.

Table 18: Types of NPOs including risk ratings

NPO type	Number of banks that banked the NPOs	Majority risk rating
Religious organisations	12	Mostly medium
Clubs	2	Mostly high
Social, social welfare, community or informal bodies	8	Low to high (single risk rating could not be determined)
Associations	4	Low to medium
Schools	5	Low to medium
Foundations	5	Mostly high
Body corporates	2	Medium to high
Trusts	4	Mostly high
Charitable organisations	7	Low to high (single risk rating could not be determined)
Youth movements	1	Medium to high
Drug rehabilitation centres	1	Medium to high
Orphanages	1	Medium to high
Embassies, missions and consulates	1	Low
Sporting organisations	4	Medium to high
Professional bodies	1	Medium
Political parties	1	Medium
Burial societies	1	Medium
Companies	7	Medium to high

8.1.11.2 Number of NPOs

Table 19: Total number of NPOs[14]

Categories of banks	Number of banked NPOs	Percentage of banked NPOs	Number of unregistered banked NPOs	Unregistered banked NPOs as a percentage of total banked NPOs
Large banks	58 129	61.528%	36 388	38.515%
Medium to small locally controlled banks	36 139	38.252%	31 933	33.801%
Branches of foreign banks and foreign controlled banks	204	0.216%	162	0.171%
Mutual banks	4	0.004%	1	0.001%
Total	**94 476**	**100%**	**68 484**	**72.488%**

It is evident from Table 19 that most NPOs were banked by the large banks, as follows:

- bank one banked 41.7%;
- bank two banked 12.9%; and
- bank three banked 15.2% of these clients.

Locally controlled banks banked the second-most NPOs, divided as follows:

- bank one banked 90.2%;
- bank two banked 1.5%; and
- bank three banked 0.6% of these clients.

[14] Registered with the Department of Social Development and unregistered

Foreign branches banked 0.21% of NPOs across the sector, with one foreign branch banking the vast majority of NPOs at 81.37%. Lastly, mutual banks only banked three NPOs.

Additionally, Table 19 indicates that 72.5% of NPOs were unregistered across the sector. The majority of unregistered NPOs were banked by the large banks, with one large bank banking 37.85% of unregistered NPOs across the sector. One large bank banked 98.3% of unregistered NPOs within the subsector. Locally controlled banks banked 33.8% of unregistered NPOs, with one locally controlled bank banking 98.98% of these unregistered NPOs within the subsector. Only 0.17% of unregistered NPOs were banked within the foreign branches subsector, with one foreign branch banking 93.2% of unregistered NPOs within the subsector. Lastly, the mutual banks subsector only banked one unregistered NPO.

The impact of such a high volume of NPOs being banked, especially the number of unregistered NPOs, leads one to question the due diligence measures employed by such entities and the necessity for stronger legal frameworks to address unregistered NPOs. NPOs have traditionally always been viewed as being susceptible to abuse for ML and TF[15]. It is thus important to ensure that the activities of NPOs are well understood, including their size, activities, destinations involved, and potential funders and beneficiaries.

[15] FATF – Combating abuse of non-profit organisations

8.1.11.3 Number of high-risk NPOs

Table 20: Total number of high-risk NPOs[16]

Categories of banks	Number of banked NPOs	Number of banked NPOs rated as high risk	Percentage of high-risk NPOs as a total of banked NPOs
Large banks	58 129	1 063	1.125%
Medium to small locally controlled banks	36 139	426	0.451%
Branches of foreign banks and foreign controlled banks	204	16	0.017%
Mutual banks	4	1	0.001%
Total	**94 476**	**1 506**	**1.594%**

From Table 20, it is evident that 1.59% of the total number of NPOs banked across the sector were high risk. Most high-risk NPOs were banked within the large banks subsector (1.13% of the total number of banked NPOs). Two large banks banked the most high-risk NPOs within their subsector at 66.4% and 23.5%, respectively. The locally controlled banks banked the second-most high-risk NPOs at 0.45% of the total banked NPOs. Two locally controlled banks banked 44.6% and 25.1% of the high-risk NPOs within their subsector, respectively. Only four foreign branches banked high-risk NPOs, amounting to 0.017% of the total number of banked NPOs, and only one high-risk NPO was banked within the mutual banks subsector.

[16] One large bank mentioned that one of their business units were unable to distinguish between registered and unregistered NPOs.

8.1.11.4 Number of foreign-owned NPOs

Table 21: Total number of foreign-owned NPOs

Categories of banks	Number of banked NPOs	Number of foreign-owned NPOs	Foreign-owned NPOs as a percentage of total banked NPOs
Large banks	58 129	102	0.108%
Medium to small locally controlled banks	36 139	0	0%
Branches of foreign banks and foreign controlled banks	204	5	0.005%
Mutual banks	4	3	0.003%
Total	**94 476**	**110**	**0.116%**

Table 21 shows that the 0.16% of the total number of NPOs banked across the sector was foreign-owned. Most foreign-owned NPOs were banked by the large banks (0.11% of the total number of NPOs banked). Two large banks banked the most foreign NPOs within their subsector, at 48.7% and 45.1%, respectively. The locally controlled banks did not bank any foreign-owned NPOs, while three foreign branches and one mutual bank banked these NPOs.

8.1.11.5 Number of NPOs operating in high-risk jurisdictions

Table 22: Total number of NPOs operating in high-risk jurisdictions

Categories of banks	Number of banked NPOs	Number of NPOs operating in high-risk jurisdictions	Number of NPOs within high-risk jurisdictions as percentage of total banked NPOs
Large banks	58 129	157	0.27%0.166%
Medium to small locally controlled banks	36 139	0	0%
Branches of foreign banks and foreign controlled banks	204	0	0%
Mutual banks	4	0	0%
Total	**94 476**	**157**	**0.166%**

All NPOs that operated in high-risk jurisdictions were banked by the large banks. One large bank had 94.3% of these NPOs as clients. Given the lack of oversight and supervision over NPOs (registered or unregistered), the high volume of NPOs banked by the large banks and the propensity for NPOs to be used to facilitate the proceeds of crime, the risk of ML/TF is high when dealing with these types of clients.

8.2 Common vulnerabilities linked to clients

The following common vulnerabilities are linked to clients identified by banks:

- incorrect client risk rating due to data inaccuracies and incomplete CDD information;
- challenges in establishing beneficial ownership, which is still in its infancy stages in South Africa, such as the absence of a central country registry;
- third-party fund administrators as clients, where reliance is placed on the third party to identify and verify clients;
- clients' transactions not falling within the expected monthly turnover that was established when the account was opened;
- accounts used for illegal investment schemes, such as pyramid schemes and Ponzi schemes;
- abuse of accounts for minors (individuals younger than 18 years) and misuse of estate late accounts
- ageing client base susceptible to fraud and phishing scams;
- account take-overs where fraudsters can take over someone's account without their knowledge;
- misuse of individual accounts as business accounts;
- complex ownership structures used to hide the true identity of sanctioned parties;
- high-net-worth individuals using investment accounts to conceal illicit proceeds;
- identification and verification of authority when dealing with foreign governments and sovereign entities;
- the increase in clients involved in high-risk industries such as mining, export or imports;

- traditional ML/TF/PF vulnerabilities involving relationships with PEPs, bribery and corruption, trade-based money laundering and high-risk cross-border banking;
- identification of cryptocurrencies and exchanges (as client types); and
- misuse of charitable organisations or NPOs, complicated companies and trusts.

8.3 Banking sector risk rating of client risk

Table 23: Client risk category

Large banks	Medium to small locally controlled banks	Branches of foreign banks and foreign controlled banks	Mutual banks
High	High	High	Low

Overall risk: High – The sub-risk factor (client risk) was assigned a weighting, and an average risk score was determined for each of the four banking categories. Each sub-risk category was weighted, and an average risk score determined the overall risk rating for the subsector. The overall risk rating score and the percentage weight per the subsector was used to calculate the overall risk rating.

9. Product inherent risk assessment

This section focuses on the assessment of the qualitative responses and quantitative data collected from the banking sector in respect of their product offerings. The analysis aims to provide a holistic view of the areas of concern and common practices in the banks.

9.1 List of high-risk products prone to ML/TF abuse

The banking subsectors provided a spectrum of different products that were rated as high risk and matched a list of products prone to ML/TF abuse. These are:

- trade finance products and services;
- cash-intensive transactions;
- cross-currency transactions;
- correspondent banking;

- investment products;
- treasury products;
- corporate finance;
- credit products;
- trust accounts; and
- stokvel accounts.

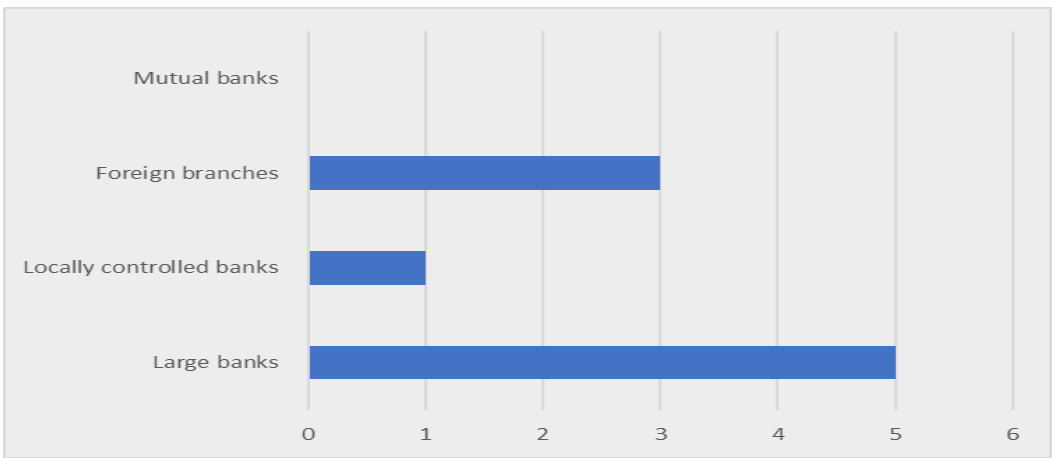
Although each bank uses different terms for these products and services, these were the main products identified as high risk.

Trade finance products have proven to be prone to abuse relating to ML and TF. Some banks mentioned that all high-risk products and services categories were deemed to be prone to ML abuse because of their transactional features and/or capabilities, cross-border capabilities, acceptance of cash and transformation of funds held with the bank into cash, ability of unverified parties to deposit funds and receive payments, and enabling transactions through remote access.

9.2 Products or services without limits on cash withdrawals in other jurisdictions

Only a few of the banks offer products and services without limits on cash withdrawals in other jurisdictions, as shown in Figure 3.

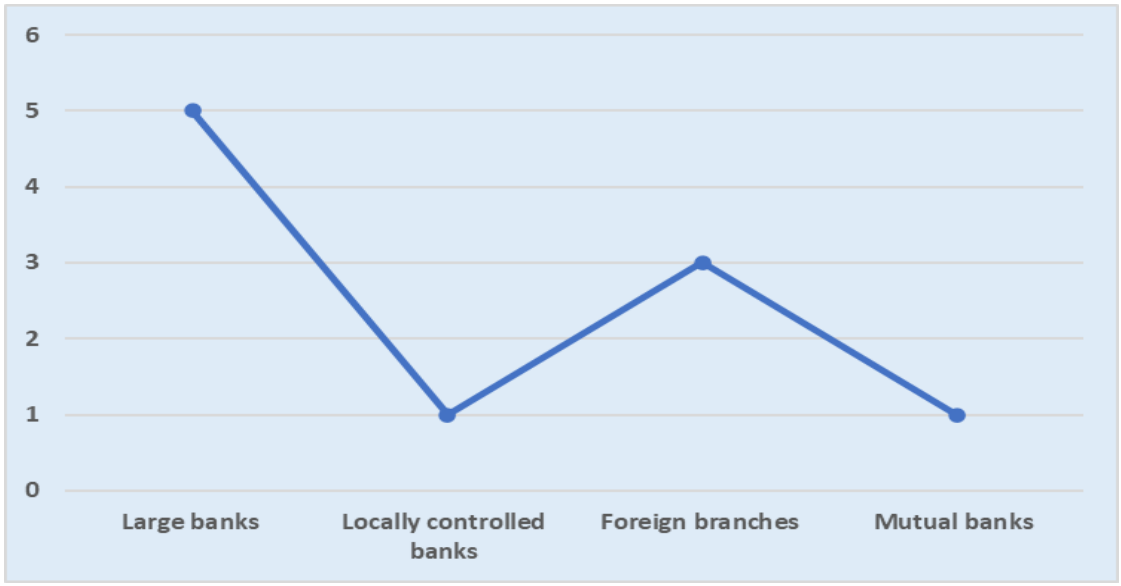
Figure 3: Products or services without limits on cash withdrawals in other jurisdictions



9.3 Products or services without limits on cash withdrawals locally

Similarly, only a few banks offer products and services without limits on cash withdrawals locally, as shown in Figure 4.

Figure 4: Products or services without limits on cash withdrawals locally



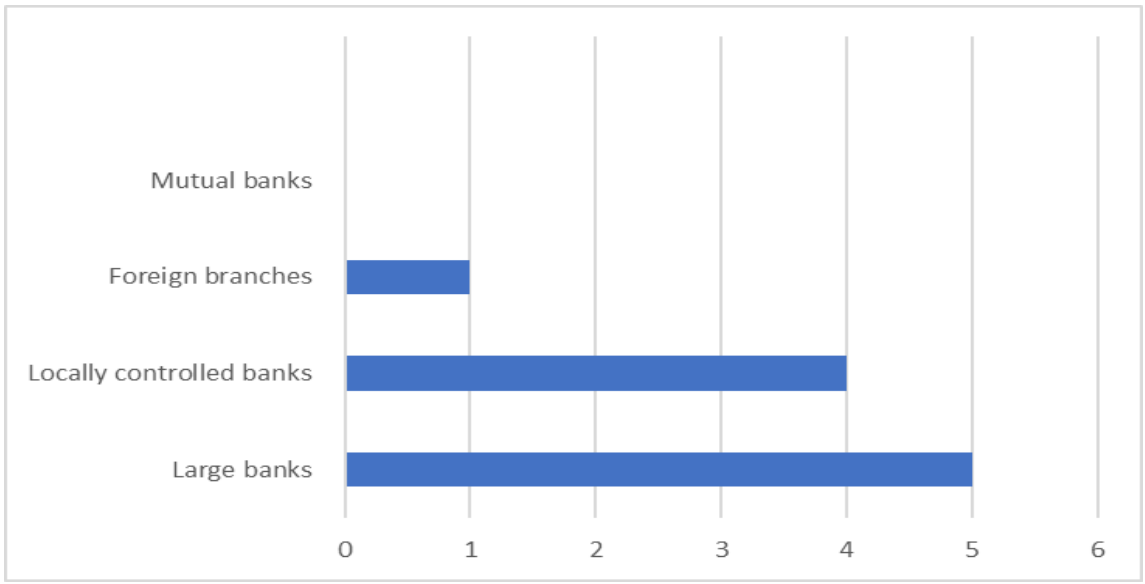
The following products without limits on cash withdrawals locally were listed:

- cheque accounts;
- credit cards;
- private bank accounts;
- business accounts;
- investments; and
- money market.

9.4 Products that allow the use of multiple cards

Only a few of the banks offer these products and services, as shown in Figure 5 on the next page.

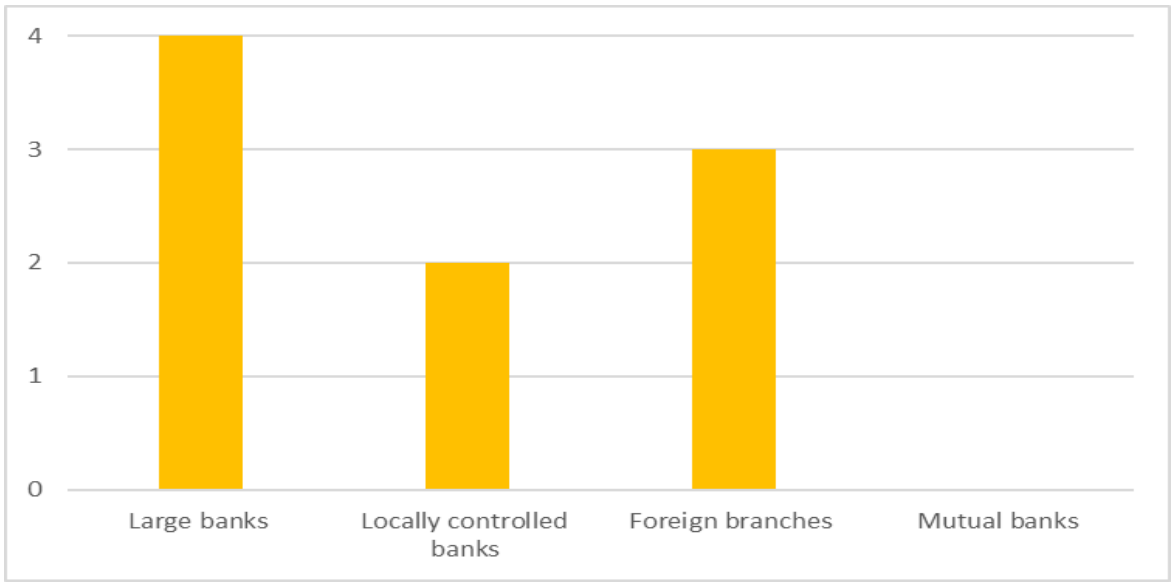
Figure 5: Products that allow the use of multiple cards



9.5 Money remittance services for banked clients

The banks that did not hold Authorised Dealer licences indicated that they did not offer these products. Based on the feedback received from the banks, only a few of the banks provide money remittance services for banked clients.

Figure 6: Money remittance services for banked clients



Common themes and similarities

The banks listed product offerings relating to money remittance services for banked clients, which included:

- instant money transfer;
- money remittance;
- cross-border money transfer services through retail shops;
- domestic money services through retail shops; and
- telegraphic transfers.

9.6 Money remittance services for non-banked clients

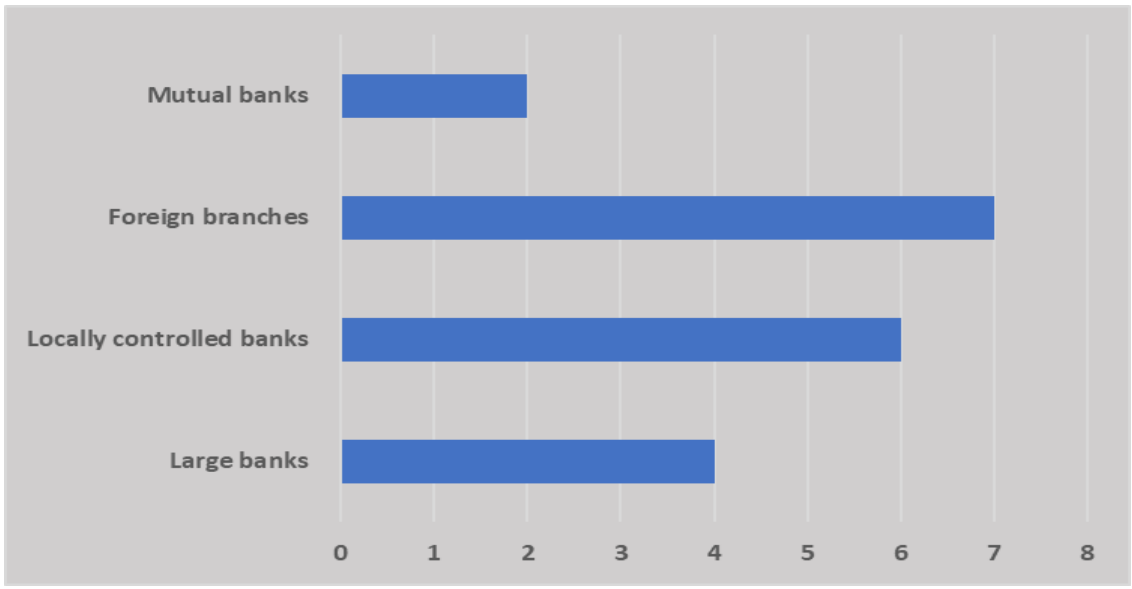
Three of the large banks provided this service. One large bank indicated that the same remittance products were available to both banked and non-banked clients. Banks face a few risks when engaging with non-banked clients and offering money remittance services, such as:

- Digital services: The growth of digital remittance services and technology has led to the emergence of new ML risks. Online money remittance services make it easier for criminals to circumvent identity verification processes, especially the remittance services for the non-banked clients.
- Prepaid cards: Some prepaid payment cards can be used to send and receive money and to withdraw cash from ATMs with funds loaded anonymously over the internet.
- Money mules: The anonymity associated with remittance services means that money launderers can engage third parties to conduct transactions on their behalf.

9.7 Non-face-to-face products offered by the banks

Based on the feedback received from the banks, 13 banks indicated that they did not offer any non-face-to-face products, while two banks indicated that all their products were only offered remotely (rather than face to face).

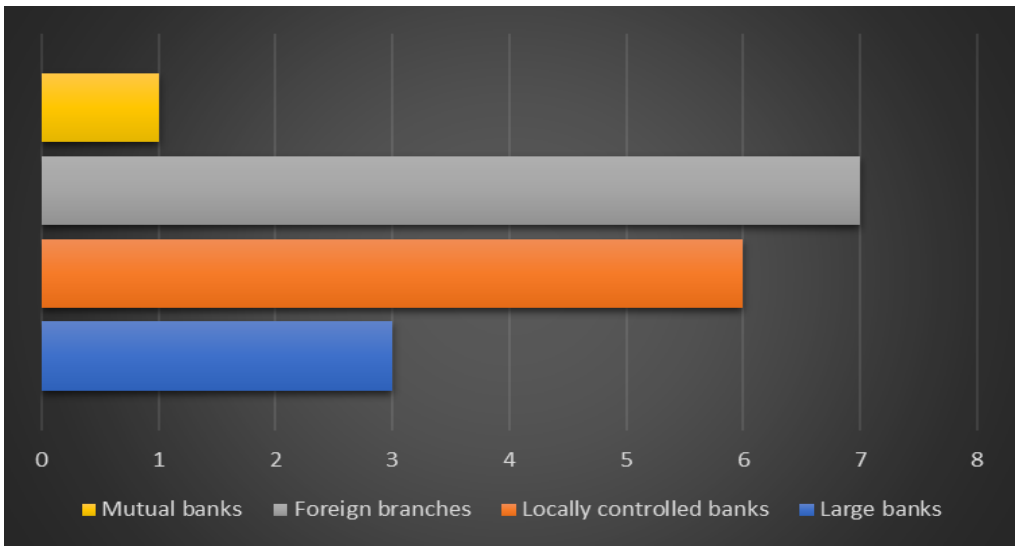
Figure 7: Non-face-to-face products offered by banks



9.8 Products that involve transactions of large amounts of cash

Based on the feedback received from the banks, 13 banks indicated that this was not applicable as they did not deal with large amounts of cash.

Figure 8: Products that involve transactions of large amounts of cash



Common themes and similarities

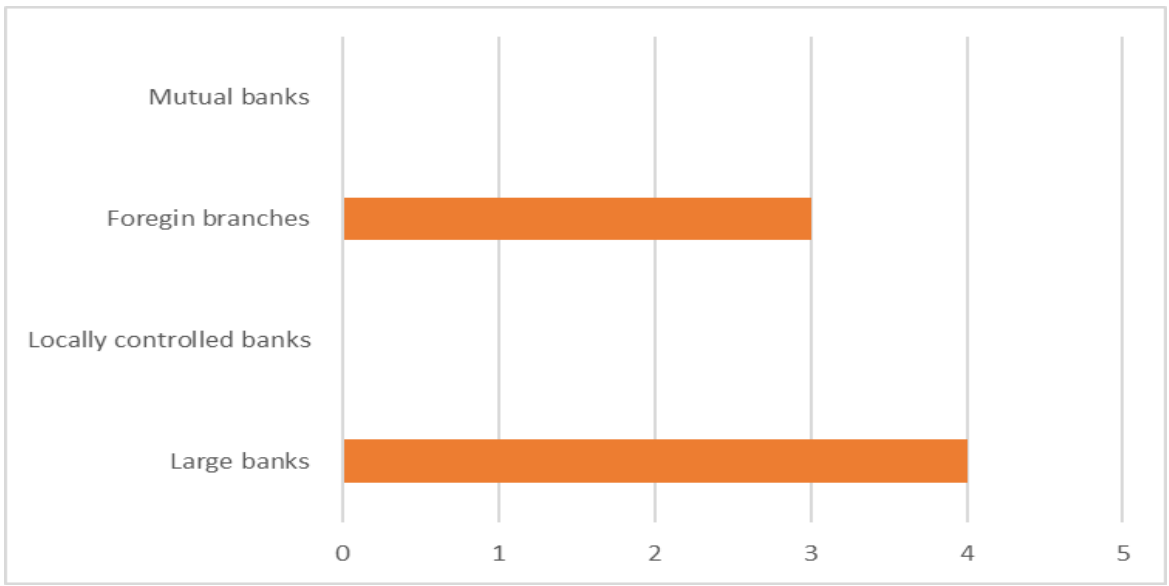
The banks listed the following products:

- fixed deposits;
- loans;
- transactional accounts;
- credit cards;
- investments; and
- stokvel accounts.

9.9 Products or services traded in secondary markets

Twenty-one banks responded that they did not offer any products and services traded in the secondary markets.

Figure 9: Products or services traded in secondary markets



Common themes and similarities

The following products were listed by banks:

- foreign exchange trading spot;
- foreign exchange derivatives forwards;
- foreign exchange derivatives futures; and
- foreign exchange derivatives options.

9.10 Common vulnerabilities linked to products

The following common vulnerabilities are linked to products identified by banks:

- money value transfer services offered in conjunction with partners or as part of a joint venture, as these products are available to non-residents and enable cross-border movement of funds;
- retail foreign exchange products (such as foreign currency, foreign currency accounts and forex payments);
- trade finance (over-invoicing of the financed asset or fraudulent transactions);
- prepaid card products, such as for micro-lending, pay-cards (ATM, point of sale, salaries, petty cash or any cash payments) and gift cards;
- travel wallets for local and foreign travel;
- foreign exchange products (lack of knowledge of the client due to reliance on brokers); and
- transactional banking (digital onboarding resulting in the opening of fraudulent bank accounts)

9.11 Products and services risk category

Table 24: Products and services risk category

Large banks	Locally controlled banks	Branches of foreign banks and foreign controlled banks	Mutual banks
High	Medium	High	Low

Overall risk: High – The sub-risk factor (products and services) consists of threats, vulnerabilities and high-risk areas identified. The sub-risk factor was assigned a weighting, and an average risk score was determined for each of the four banking categories. Each sub-risk category was weighted, and an average risk score determined the overall risk rating for the subsector of the risk factor. The overall risk rating score and the percentage weight per the subsector was used to calculate the overall risk rating.

The PA concluded on the above product ratings stemming from the information received from the banking sector. The outcome was determined taking into account the various products and/or services that are offered by the banks and bearing in mind ML/TF risks associated with those products.

10. Delivery channels

This section focuses on the assessment of the responses and the PA's experience in the banking sector relating to inherent ML/TF risks in the different delivery channels used by banks.

The banking sector's products and service delivery channels have evolved over time. The typical use of face-to-face or in-branch visits by clients as a delivery channel has decreased greatly, while contactless or remote and virtual onboarding of clients has increased. The COVID-19 pandemic has also affected the use of face-to-face banking channels within the sector.

10.1 Internet banking and mobile banking

Over 90% of the banking sector offers online banking services (internet banking) or mobile application banking (using technological applications), with the exception of one mutual bank.

Three of the newest South African banks primarily use mobile application banking, with no physical branches for their clients. These platforms increase the ML/TF vulnerabilities, as the banks face the risk of being unable to reliably identify and verify clients through remote or digital onboarding processes. Although online banking offers faster transactions and more convenient options for banking, these features are also attractive to criminals. Online features can hide the true identity of clients (,which in-branch visits would have detected), and these features can also hide the true destination and beneficiaries of funds.

10.2 Automated teller machines

From the feedback received, 35% of banks have ATM facilities: this includes 33% of the large banks, 50% of locally controlled banks, 17% of branches of foreign banks and subsidiaries, and none of the mutual banks. Some advanced ATMs accept cash deposits, which limits identification of the client and the source of funds. Criminals use ATMs to place the proceeds of crime into the banking system, which increases the ML/TF vulnerabilities for the whole sector.

10.3 Banking agency relationships

The banks allow their clients to conduct some transactions, such as cash deposits or withdrawals, through the branches or ATMs (withdrawals only) or money services outlets of other banks and or third parties. This process is known as agent banking. All subsectors are using these services with third parties. Agent banking relationships provide access to accounts, including for clients in remote areas. However, this service can increase the length of a transaction chain due to the third-party process. The agent banking relationship can also make it difficult for the suspicious and unusual transactions monitoring and governance of ML/TF risk if not clearly agreed upon in the agent banking relationship agreement.

10.4 Summary of analysis based on the responses from the banks

Table 25: Summary of banks' responses on delivery channels

		Responses of the banks			
		Large banks	**Locally controlled banks**	**Foreign branches and foreign controlled banks**	**Mutual banks**
No.	Description				
1.	Products or services offered to prospective clients through intermediaries or third parties	Over 30 products	Average of three products	Five products	Two products

2.	Number of clients onboarded through digital channels (as opposed to face-to-face)	More than 2 000 000	Average of 3 000 000	Average of 1 000	Average of 2 000
3.	Number of products offered through digital channels (i.e. non-face to face versus products offered on face-to-face basis)	Majority of products were offered face-to-face.	The two digital banks offer all products through digital channels. Traditional banks offered most products face-to-face, although some used both platforms, with the majority being face-to-face.	A total of 12 banks did not offer products through digital channels. Two banks offered all products through digital channels. Three banks offered products using both channels.	Two mutual banks offered a total of seven products through digital channels. One mutual bank did not offer any products through digital channels.
4.	Number of cybercrime and online fraud attacks or attempts in the last 24 months	40–217 incidents of cybercrime and online fraud.	1 237 incidents of cybercrime and online fraud attempts, which relates to an averaged 137 incidents per bank Three of the nine banks did not have any attacks. The digital banks had fewer incidents of cybercrime or online fraud compared to the traditional banks.	10 banks had not experienced any cybercrime or online fraud attempts. Three banks had one to two attempts. Two banks had 56 attempts. One bank had 664 attempts.	No cybercrime and online fraud attacks or attempts.

5.	Amount of funds lost due to cybercrime or online fraud attacks in the last 24 months	Net losses totalled R322.1 million.	Total losses of about R159.1 million, of which R7.9 million was due to staff collusion. One of the digital banks had the lowest number of losses.	None.	None.
6.	Number of successful cybercrime or online fraud attacks against the institution or its clients	24 091.	847. One of the nine banks did not know how many attempts were successful, indicating weak controls.	None.	None.
7.	Frequency of communication with clients on alertness or education against cybercrime or online fraud	Banks with real-time fraud awareness had the least number of cybercrime and online fraud cases, whereas banks with monthly or less frequent fraud communications to clients had the highest cases. More real-time communication is likely to reduce the cybercrime and online fraud attacks significantly as the clients are alerted constantly.	Frequency of alert communication with clients ranged from unspecified regular intervals to monthly. One out of the nine locally controlled banks did not have alert communications.	Four banks did not communicate with clients on this matter. Eight banks communicated on an ad-hoc basis and provided information on their websites.	Two banks did not communicate with clients on this matter. One had a process in place to create alertness against cybercrime and online fraud when required.
8.	Trend analysis or comparison (before and after) in the number of cybercrime or online fraud	No trend analysis conducted.	No trend analysis conducted. One bank indicated that the trends were changing due to	No trend analysis conducted.	One bank said no trend observed. Two banks said none.

	cases against clients since the implementation of awareness against cybercrime and online fraud attacks		new fraud scams developing as a result of COVID-19.		

10.5 Common vulnerabilities linked to delivery channels identified by banks

Banks highlighted the following vulnerabilities linked to delivery channels:

- digital delivery channels pose a greater risk of not identifying the true client – either at the onboarding or the transactional phase;
- indirect delivery channels rely on a third party to collect client onboarding and/or transactional information;
- rapid movement of funds through electronic funds transfer (EFT) and real-time clearing;
- the use of cards outside South Africa;
- non-face-to-face client interactions and distribution channels;
- internet banking; and
- internet or online gambling.

10.6 Delivery channels risk category

Table 26: Delivery channels risk category

Large banks	Locally controlled banks	Branches of foreign and foreign controlled banks	Mutual banks
High	**High**	**High**	**Medium**[17]

[17] One mutual bank offers its products and interacts with its clients digitally.

Overall risk: High – The sub-risk factor (delivery channels) consists of threats, vulnerabilities, high-risk areas identified, and some elements discussed above. The sub-risk factor was assigned a weighting, and an average risk score was determined for each of the four banking categories. Each sub-risk category was weighted, and an average risk score determined the overall risk rating for the subsector. The overall risk rating score and the percentage weight per the subsector was used to calculate the overall risk rating.

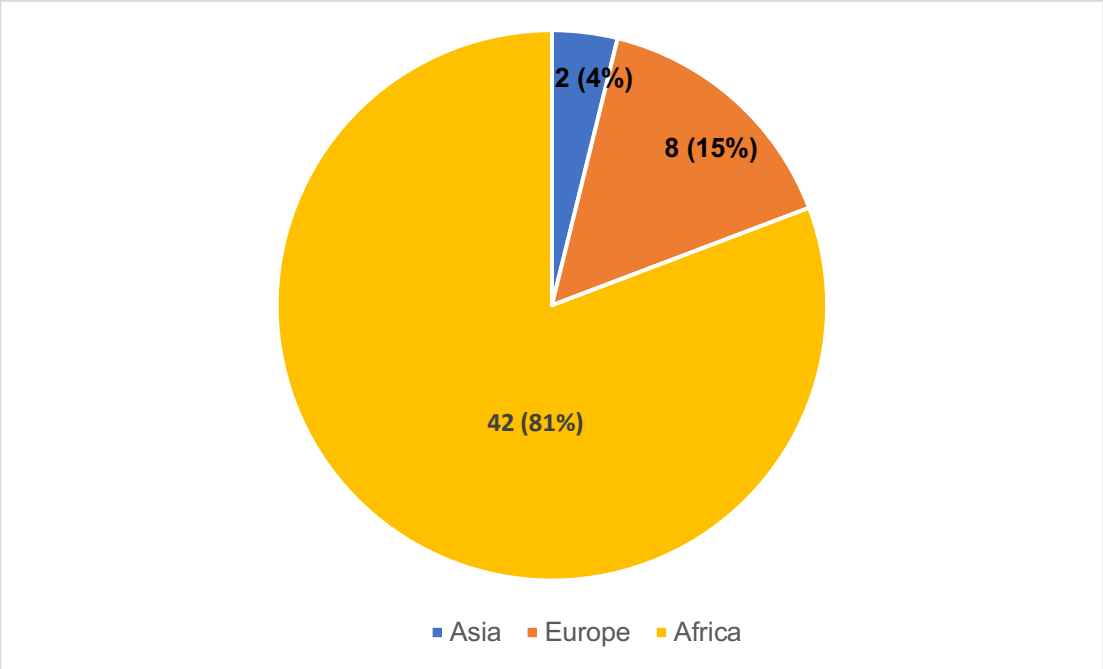
11. Geography

This section focuses on the assessment of qualitative responses from the banking sector in respect of their geographic risk exposure. The assessment aims to provide a general view of the geographic risk as the implemented controls were the same across all four banking subsectors.

11.1 South African banks and global footprint

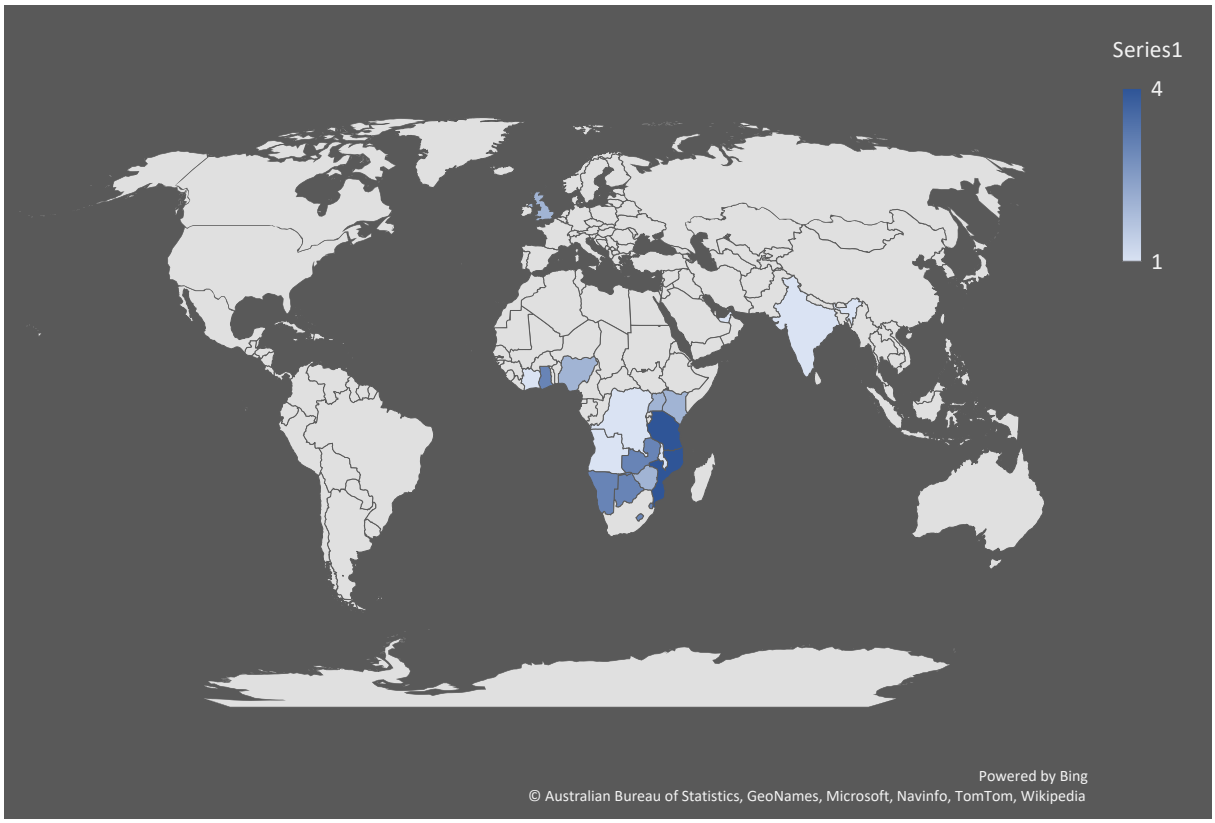
In terms of section 52 of the Banks Act 94 of 1990 (Banks Act), South African banks can acquire or establish cross-border interests, including banking subsidiaries, branches, or representative offices. As at October 2021, South African banks were operating in 52 cross-border banking operations in 25 countries across 3 continents. This is summarised in the next two figures.

Figure 10: South African banks operating globally[18]



[18] Forms BA600 – Regulations relating to Banks.

Figure 11: Footprint of licenced South African banks[19]



11.2 Jurisdictions with strategic deficiencies

Table 27 shows jurisdictions where South African banks have a presence that the FATF has flagged as jurisdictions with strategic deficiencies and/or jurisdictions no longer subject to increased monitoring, implying that they carry increased risk.

Table 27: FATF jurisdictions with strategic deficiencies[20]

Jurisdictions with strategic deficiencies (as at October 2021)	Jurisdiction no longer subject to increased monitoring (as at October 2021)
• South Sudan • Uganda	• Botswana • Mauritius

[19] Forms BA600 – Regulations relating to Banks.

[20] When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the 'grey list'. Documents – FATF (fatf-gafi.org)

11.3 Results of the assessment

Table 28 reflects the top five high-risk jurisdictions where clients of South African banks are domiciled.

Table 28: List of top five high-risk jurisdictions in respect of clients

Banking categories	Top five countries
Large banks	Zimbabwe Mozambique Mauritius Nigeria Democratic Republic of Congo
Locally controlled banks	Zimbabwe Mozambique Mauritius Nigeria Democratic Republic of Congo
Branches of foreign banks or foreign-controlled banks	Mauritius Nigeria Uganda Zimbabwe Mozambique
Mutual banks	Zimbabwe

In terms of large banks, 157 NPO clients were found to be operating in high-risk jurisdictions. None of the other categories of banks had NPO clients operating in high-risk jurisdictions. A foreign branch situated in South Africa's international footprint highlighted operations in Nigeria and Mauritius[21]. No locally controlled banks or mutual banks had operations in countries outside South Africa. Two of the 34 banks confirmed that they had operations in high-risk jurisdictions subject to sanctions.

[21] Countries treated as high risk at a point in time

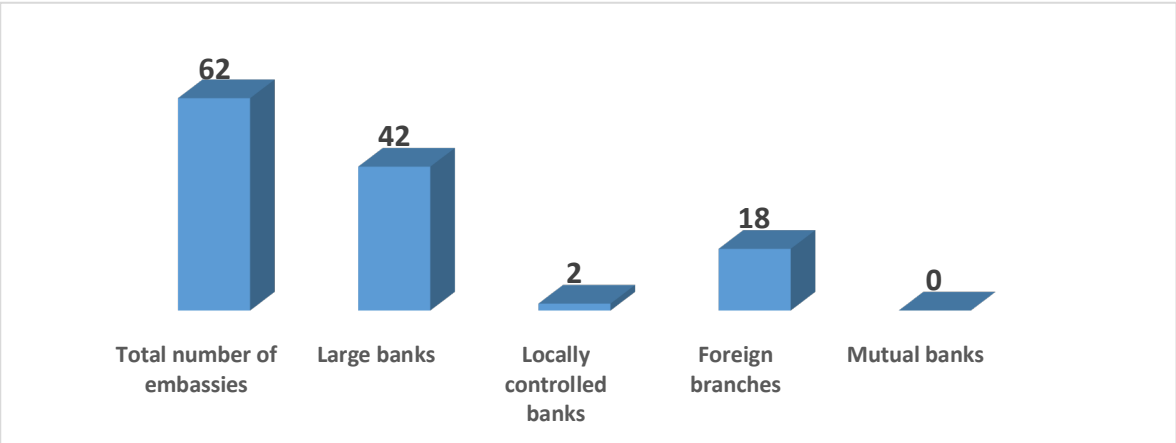
Large banks and foreign banks indicated that the types of products offered to clients in high-risk jurisdictions would be conditional on the client qualifying for the product. The locally controlled banks and mutual banks indicated that they did not provide a specific list of products to clients in high-risk jurisdictions. This poses a risk to the banking sector as locally controlled banks might be providing products and services to clients in countries with weak AML/CFT controls.

Three out of the 34 banks indicated that the following jurisdictions, from which clients are onboarded, apply excessive client confidentiality provisions. This makes it difficult or impossible to obtain certain client information, such as on beneficial ownership:

- South Korea;
- eSwatini;
- Seychelles;
- United Arab Emirates;
- Mauritius;
- United Kingdom; and
- European Union countries

Figure 12 shows that 62 embassies were banked across the different categories of banks.

Figure 12: Number of embassies banked



The five large banks banked the highest number of embassy clients. Embassies are considered to be a higher risk as PEPs may be linked to embassies and embassy accounts, or personal accounts of embassy officials may be used for illegitimate purposes.

11.4 Banking sector's geographical risk

Table 29: Geographical risk by category

Large banks	Locally controlled banks	Branches of foreign banks and foreign controlled banks	Mutual banks
High	Medium	High	Low

Overall risk: High – The sub-risk factor (geographic risk) is made up of threats, vulnerabilities, high-risk areas identified, and some elements discussed above. The sub-risk factor was assigned a weighting, and an average risk score was determined for each of the four banking categories. Each sub-risk category was weighted, and an average risk score determined the overall risk rating for the subsector. The overall risk rating score and the percentage weight per the subsector was used to calculate the overall risk rating.

12. Threat environment[22]

Globally, the banking sector has always attracted significant scrutiny on ML/TF matters. This happens because the banking sector is key to transacting and facilitating the payment of funds from one person to another, domestically and across borders, and the volumes of transactions and flow of funds are large and fairly quick.

[22] A threat is a person or a group of people, object or activity which has the potential to cause harm to, for example, the state, society or the economy. In the ML/TF context, this includes activities, criminals, terrorist groups and their facilitators, their funds, and past, present and future ML/TF activities and events.

12.1 Threats within the banking sector

The PA engaged with all the banks, including the five large banks, to gain a greater understanding of the key ML/TF threats banks face. The five large banks mentioned the following as the top ten ML/TF threats.

Table 30: Top 10 threats identified by large banks[23]

	Bank A	Bank B	Bank C	Bank D	Bank E
1	Bribery and corruption	Fraud	Bribery and corruption	Corruption risk and association with state capture	Corruption
2	Illicit financial flows overseas	Tax evasion	Complex structures	Increased financial crime risk	State-owned entities
3	Sophisticated international syndicates and terrorist groups	Cross-border transactions	Tax evasion	Exposure to DPIPs, FPPOs and associates	Government tenders
4	Cash-based economy	Pyramid and Ponzi schemes	ML/TF through NPOs	Cybersecurity risk	Cybercrime
5	Cybercrime and emerging technologies (cryptocurrency)	Forgery and scams	ML/TF through religious organisations	Exposure to higher risk jurisdictions	PEPs
6	Drug trafficking	Credit card application fraud (South African Banking Risk Information Centre)	Cryptocurrency	Exposure to higher risk industries	High-risk clients
7	Human trafficking and modern-day slavery	Wildlife trafficking	Shipping/trade-based ML	Crypto and virtual assets	Trade-based ML
8	Environmental crimes	Advanced payments	Terrorism financing	Trading in illegal narcotics, illegal wildlife	Cash

[23] In no particular order

	Bank A	Bank B	Bank C	Bank D	Bank E
				trafficking	
9	Precious metals and minerals smuggling	Deviation from onboarding agreement	Illegal wildlife trade	Poaching and human trafficking	Fraud (internal and external)
10	Tax offences		Environmental crimes	Correlation risk	419 scams

The other three banking subsectors identified similar threat areas to the aforementioned and additionally provided the following:

- non-disclosure of beneficial owners and related parties;
- cybercrime and emerging technologies, especially as no specific laws or regulations currently govern the use of emerging technologies;
- illegal investment schemes (Ponzi/pyramid), which are likely where a lot of funds from different individuals are sent to particular account holders;
- the movement of funds across borders, such as remittance transactions;
- kidnapping for ransom is often used to finance terrorism-related activities;
- illicit financial flows, such as cash received into accounts and immediately transferred outward;
- COVID-19-related financial crime that emerged through irregular expenditure linked to personal protective equipment;
- trade-based ML, such as non-compliance with customs and export requirements, use of fake or fraudulent documents related to shipping or customs, or payments to facilitate transactions or trade finance;
- risks posed by unregulated entities such as NPOs, which present vulnerabilities that can be exploited in the context of voluntary registration;
- activities of criminal syndicates, including the use of mule accounts and account takeovers; and
- state-owned entities and government tender fraud.

13. Vulnerabilities

The PA analysed the banks' survey responses and compared the types of predicate offences that result in ML.

13.1 Common themes

Certain common vulnerabilities were identified across all four subsectors, including:

- an inability to identify DPIPs;
- the inability of banks to obtain beneficial ownership information;
- the offering of trade finance products and services;
- an inability to identify cryptocurrencies and exchanges (as client types);
- non-face-to-face client onboarding and interactions;
- products that allow large volumes of cash deposits;
- the lack of a single client view throughout a bank;
- an increase in cybercrime and the use of sophisticated technology; and
- various data issues, such as misalignment, inaccuracies and integrity of data.

13.2 Banking sector's risk of other risk factors by category

Table 31: Risk of other risk factors, including vulnerabilities, by category

Large banks	Locally controlled banks	Branches of foreign banks and foreign controlled banks	Mutual banks
High	High	High	Low

Overall risk: High – The sub-risk factor (other risk factors) comprises of threats, vulnerabilities, high-risk areas identified, and some elements discussed above. The sub-risk factor was assigned a weighting, and an average risk score was determined for each of the four banking categories. Each sub-risk category was weighted, and an average risk score determined the overall risk rating for the subsector. The overall risk rating score and the percentage weight per the subsector was used to calculate the overall risk rating.

14. Proliferation financing risk

This section focuses on the assessment of qualitative responses from the banking sector in respect of PF risks.

14.1 Population and sample size

To assess the banks' understanding of their risks relating to PF, weapons of mass destruction and/or an exposure to dual-use goods[24], the PA considered the responses provided by the banks in respect of the period from 1 October 2018 to 31 December 2020.

14.2 Results of assessment

14.2.1 Banking relationships with diplomats, consular staff and missions

One bank confirmed a client relationship with two diplomats/consular staff and/or missions from North Korea or Iran.

14.2.2 Mechanisms to detect transport to or from North Korea or Iran

From the feedback received, 19 out of the 34 banks (56%) stated that they had implemented detection mechanisms with respect to vessels, aircraft or crew services to or from North Korea or Iran, which was predominantly sanctions-screening controls. Table 32 provides more details of the analysis.

Table 32: Detection methods

Response	Number of banks
Not applicable – the bank only operated within South Africa or did not deal with import/export payments	14
Would not establish a business relationship with North Korea and Iran	1

[24] Dual-use goods are items that have both commercial and military or proliferation applications. This can include goods that are components of a weapon, or those that would be used in the manufacture of a weapon (e.g. certain machine tools that are used for repairing automobiles can also be used to manufacture certain component parts of missiles). (Ref: Page 9: FATF – Typologies Report on Proliferation Financing)

Number of banks with detection methods in place: Screening of the transaction based on the following fields (MT103): • Vessel/shipment tracking • Ports • Import and export payments • Dual-use goods	19

14.2.3 United Nations Panel of Experts reports

14.2.3.1 Use of reports

The PA noted that the Panel of Experts reports issued by the United Nations (UN), previously highlighted risks that link to South Africa. These included the linking of illegal ATM withdrawals using hacked credentials from a South African bank to a ringleader who fled from Japan to North Korea, the import of electrical equipment from North Korea to South Africa in September 2020, and the use of diplomats at the North Korean embassy in Pretoria for conducting prohibited activities in neighbouring countries.

These actual cases show that people banked as diplomats or with links to embassies could feasibly pose PF threats. However, the PA found that only 19 out of the 34 (56%) banks have taken note of and/or applied the information contained in the UN Panel of Experts reports.

Most banks indicated that they applied the information from these reports to:

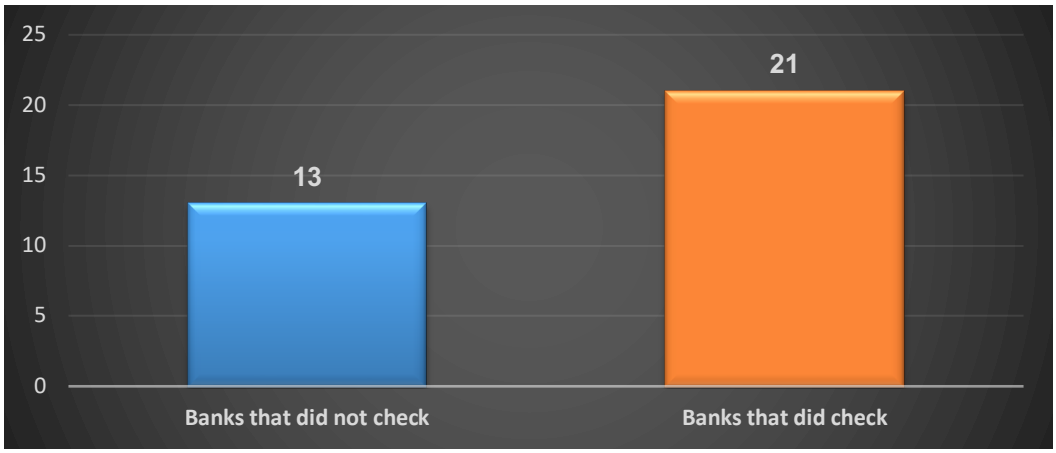
- screen for sanctions;
- incorporate it into their risk and threat assessment papers as well as risk methodologies;
- use it as a resource; and/or
- take note only.

14.2.3.2 Use of listed persons or entities in the reports

The PA found that 21 out of the 34 (62%) banks considered and/or applied the list in their monitoring and/or mitigating controls to detect whether their client relationships were listed in the report. Banks that applied the list indicated that the

reports were incorporated into their sanction-screening processes. Figure 14 summarises these results.

Figure 14: People or entities listed in the reports



Banks that do not keep abreast of these reports may be more vulnerable or at risk of serving clients with links to sanctioned entities or persons wishing to engage in illegal activities to support PF.

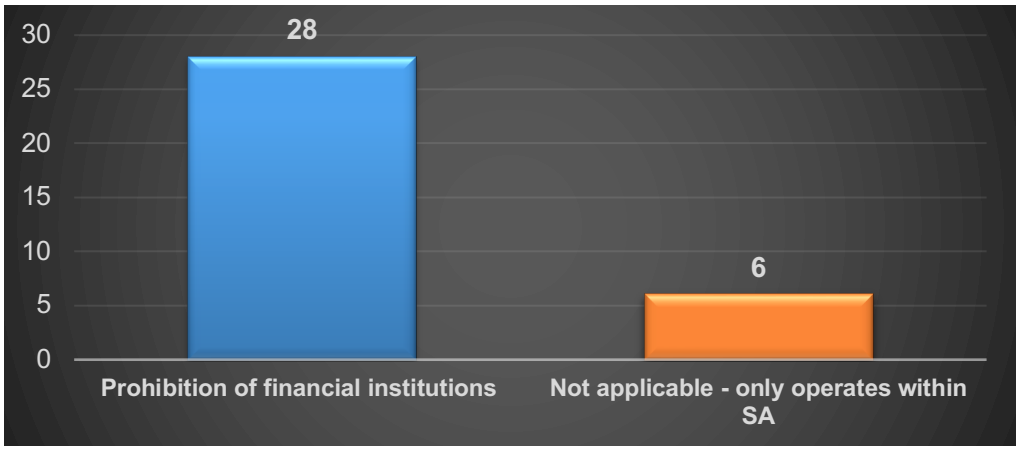
14.2.4 PF risk assessment

Based on the analysed feedback provided by the banks, 15 out of the 34 (44%) banks confirmed that they have conducted a PF risk assessment, in terms of section 42 of the FIC Act.

14.2.5 Banking relationships with North Korean and Iranian financial institutions

As shown in Figure 15, 28 out of the 34 banks (82%) confirmed that they maintained client relationships, including CBRs, with North Korean or Iranian financial institutions.

Figure 15: Number of North Korean and Iranian business relationships



14.2.6 Data used to assess PF risk exposure

The banks identified and/or assessed their possible PF risk exposure as follows:

1. 17 out of the 34 (50%) banks did not provide details on the data used to identify and assess their possible exposure to PF, weapons of mass destruction or their risk exposure to dual-use goods;
2. three out of the 34 (9%) banks relied on screening controls;
3. seven out of the 34 (21%) banks included the assessment of possible PF risk exposure as part their ML/TF risk assessment;
4. one out of the 34 (3%) banks included the assessment of possible PF risk exposure as part of their TF risk assessment; and
5. four out of the 34 (12%) banks used the following data:
    a. Peddling Peril Index;
    b. PF methodologies;
    c. UN Panel of Experts reports; and
    d. measuring export controls.

14.2.7 PF risks identified

Nine out of the 34 (26%) banks indicated that they identified PF risk factors to which they could be exposed, while 25 (74%) of the banks did not provide any details of PF risk factors identified or were not able to analyse the PF risk to which they could be exposed. Table 33 outlines the PF risks identified by the banking sector.

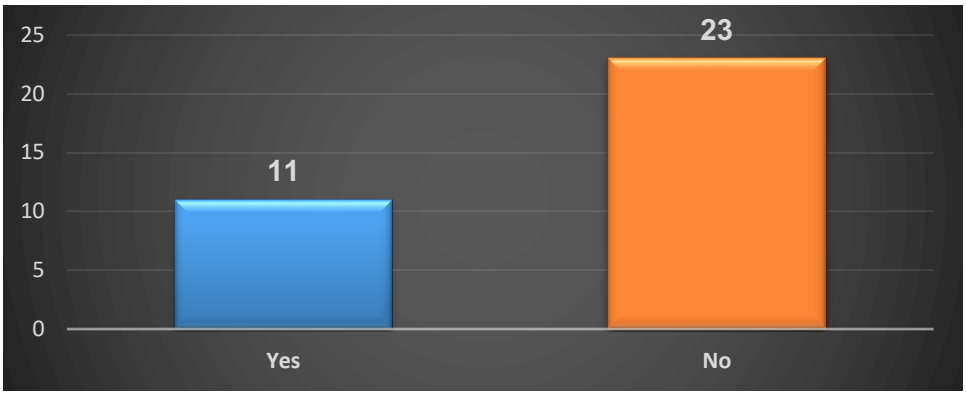
Table 33: PF risks identified within the banking sector

Risks	Total
Banks that did not identify risks, due to the nature of their clients and operations	25
Banks that did identify risks, which included: • exploitation of certain sectors in Africa (medical/construction/mining); • trade finance products; • dual-use goods; • North Korean corporate networks in Malaysia, Singapore, Hong Kong and China; • indirect payments through countries sharing a border with North Korea or Iran; • trade financing in CBRs – falsification of documentary collections and guarantees, as banks relied only on supporting documents and did not inspect the actual shipments; • corporate and investment banking in relation to international trade finance; • freight services; and • maritime business.	9

14.2.8 Risk assessment of dual-use goods

Eleven out of the 34 (32%) banks confirmed that that they have identified and assessed possible abuse of dual-use goods for the purpose of PF.

Figure 16: Identification and assessment of dual-use goods



14.2.9 Details on risk assessment of dual-use goods

The banks used the following information to conduct their respective risk assessments of dual-use goods linked to PF:

- business/enterprise risk assessment;
- import/export controls as part of transaction-screening/payment-screening;
- review of global guidance and international best practice to identify clients, industries and activities involving such goods;

- scrutiny of trade documents (bill of lading, letter of credit, bill for collection and guarantees);
- part of sanction compliance assessment; and/or
- use of the European Union website.

14.2.10 Dual-use goods susceptible to PF

From the feedback provided to the PA, it was noted that the banking industry regarded the following products/services as more susceptible to PF in respect of dual-use goods:

- medical equipment;
- tobacco products;
- alcohol;
- scrap metal;
- gems;
- jewellery;
- branded luxury goods;
- computer equipment or components;
- high-value art or store value cards;
- precious metals;
- military goods;
- oil, petrochemicals and ferrous metals;
- leather;
- military equipment[25];

[25] Including but not limited to: non-offensive military aircraft (transport, training, refuelling or manned surveillance aircraft) including helicopters; military satellites and communication systems; components, ingredients or machines used in the manufacture or assembly of defence goods; logistical, training or support services linked to military, capacity-building, humanitarian or peacekeeping operations; military infrastructure design and construction, for example, naval bases, prisons, airfields, barracks, surveillance or radar stations; military vehicles that are not weapons platforms, such as trucks, jeeps, cars and transporters; naval or ocean-going vessels (non-combat, that is supply vessels, hovercraft and coast guard); and military aircraft engines (supply, servicing and repair).

- chemicals;
- manufacture and retail;
- wholesale;
- import or export of such goods and or services, including any goods or service that may be military specification;
- nuclear;
- raw materials;
- electronics;
- telecommunications and information security;
- lasers and sensors;
- navigation and avionics;
- marine equipment;
- propulsion systems, space vehicles and related equipment; and/or
- hazardous chemicals.

14.2.11 Banking sector's PF risk category

Table 34: PF risk category

Large banks	Medium to small locally controlled banks	Branches of foreign and foreign controlled banks	Mutual banks
High	High	High	Low

Overall risk: High

15. Analysis of terrorism financing risk[26]

15.1 Analysis of the banking sector

To assess the banks' understanding of their TF risk, the PA requested data from the banking sector for the period 1 October 2018 to 31 December 2020. This section focuses on the inherent TF risk in the banking sector.

15.1.1 Results of assessment

This section focuses on the inherent TF risk identification, assessment and understanding by the 34 banks in relation to the banking sector risk responses submitted to the PA.

The banks indicated that the following financial methods were used for activities related to TF, reflected in Table 35.

Table 35: Financial methods (channels) used for TF purposes

No.	Financial methods (channels)	Number of TF-related activities or transactions per year			Total per group
		2018	2019	2020	
1	Movement of physical cash	1	7	6	14
2	Money transfers or EFTs	2	1	2	5
3	Virtual assets (e.g. bitcoin)	0	0	0	0
	Total per year	**3**	**8**	**8**	**19**

In addition, banks ranked the likelihood that the following areas would be susceptible to TF risk as:

- **likely**: export of goods and materials;
- **possible**: identified fraud and insufficient data sharing between authorities; and

[26] Analysis is limited to the banking sector's understanding of terrorism financing risk exposure.

- **less likely**: tax evasion, duty evasion in NPOs, organised crime, cash couriers, spoils of war, cryptocurrency, life insurance policies, pension funds, precious metals, and insufficient coordination and cooperation between authorities.

Finally, the analysis showed that:

- 29 out of the 34 (85%) banks stated that they follow the FATF definition of TF risk or applied an extended version thereof;
- 22 out of the 34 (65%) banks could not prove that they have identified and/or assessed TF risk; and
- 1 out of the 34 (0.2%) banks has exited client relationships due to TR risk concerns.

Table 36 shows the weighting of inherent TF risk that the PA assigned to banks within South Africa and countries where they have subsidiaries operating.

Table 36: Inherent TF risk weighting

TF risk weighting	Number of banks
High	6
Medium	3
Low	6
Not provided a weighting or rating	19
Total banks	**34**

The analysis also highlighted concerns that 65% of the banks could not show an understanding of the TF risks and/or vulnerabilities they could be exposed to and consequently would not have implemented appropriate or adequate monitoring, mitigating and managing controls. This assessment result is aligned to observations in the FATF Mutual Evaluation report.

It is also important to note that 85% of the banks confirmed that they follow the FATF definition of TF, which would include the consideration of domestic unrest, according to the FATF Mutual Evaluation assessors' interpretation.

15.2 Subsidiary returns analyses

From the foreign subsidiary AML/CFT risk returns, the PA selected a sample of banks with operations in foreign subsidiaries and requested information to assist in understanding their approach to TF risks and vulnerabilities, including controls implemented to address TF risk. This section provides an overview of the PA's observations.

Table 37: Mozambique foreign subsidiaries' TF risk understanding and controls

Factors	Mozambique
1. Risk	The banks identify TF risk through several controls, including types of products that are recognised as more likely to be abused for TF. The TF inherent risk rating is considered high due to the terror attacks that have increased in the northern region of Mozambique, where the banks have a presence and therefore can be used as a conduit to conceal terrorist activities.
2. Methodology	A standardised approach is followed in identifying and assessing TF risks. The banks have a methodology customised in terms of their legislative requirements and aligned to the respective group standards. Where a higher standard exists in Mozambican legislation, it is considered and applied accordingly. One of the banks has a group-wide risk assessment methodology that applies to all its subsidiaries.
3. Threats	Recent developments in Mozambique and neighbouring countries, which potentially increase the TF risk profile. Branches may be located in the northern province of Cabo Delgado, a region where attacks have taken place by a terrorist group with links to the Islamic State (Daesh)[27]. The highest threat is some evidence of international and/or domestic terrorist groups (including sympathisers) with the capability and intent to conduct attacks as well as regular mentions of Mozambique and South Africa in extremist messaging forums. Another major threat stems from individuals inspired by radicalised environments or through self-radicalisation, who also need to fund their

[27] ISIS-Mozambique, also known as Ansar al-Sunna (and locally as al-Shabaab in Mozambique), among other names, reportedly pledged allegiance to ISIS as early as April 2018, and was acknowledged by ISIS-Core as an affiliate in August 2019. Since October 2017, ISIS-Mozambique, led by Abu Yasir Hassan, has killed more than 1, 300 civilians, and it is estimated that more than 2 300 civilians, security force members, and suspected ISIS-Mozambique militants have been killed since the terrorist group began its violent extremist insurgency. The group was responsible for orchestrating a series of large-scale and sophisticated attacks resulting in the capture of the strategic port of Mocimboa da Praia, Cabo Delgado Province. ISIS-Mozambique's attacks have caused the displacement of nearly 670 000 persons within northern Mozambique. Source: https://www.state.gov/state-department-terrorist-designations-of-isis-affiliates-and-leaders-in-the-democratic-republic-of-the-congo-and-mozambique/

Factors	Mozambique
	activities. The Ansar al-Sunna group continues to pose the most severe security threat in Cabo Delgado.
4. Vulnerabilities	• The subsidiaries conduct business with NPOs. Non-governmental organisations (NGOs) are considered to be 'subjects at risk' in the ML framework, either as fronts for terrorist organisations that raise and transfer funds or as legitimate enterprises that indirectly support the aims of terrorist organisations. • The use of cash is considered higher risk in direct and indirect TF flows using banking platforms, because of the lack of visibility and oversight of transactions. As a result, banks are unable to identify transactions associated with terrorist-related activity.
5. Controls	i. The subsidiaries implemented their CDD modules that aid in risk-profiling a client at onboarding and on an ongoing basis. Client risk-profiling includes a higher risk weighting where the associated vulnerability to CFT is considered high. Enhanced due diligence (EDD) is applied to high-risk clients through enhanced monitoring and increased frequency of reviews. ii. Automated transaction monitoring systems may be utilised. iii. Extra vigilance in assessing the associated TF risk in the northern region is applicable. The subsidiaries must notify the appropriate regulator of any suspicious activity if there are signs of a possible terrorist offence. The Terrorist Combat Law 5/2018 refers to the duty to report suspicious transactions from Article 33 of Decree 66/2014. iv. A cross-border payments (inwards and outwards) screening system has been implemented.

Table 38: Isle of Man foreign subsidiaries' TF risk understanding and controls

Factors	Isle of Man
1. Risk	The subsidiaries allocated a medium to low risk rating in respect of TF, when balancing the threats and vulnerabilities against the controls in place.
2. Methodology	A standardised approach is followed in identifying and assessing TF risks. Each subsidiary has its own methodology customised in terms of their legislative requirements and aligned to the respective group standards.
3. Threats	Consideration and connections between the bank and a target jurisdiction, including the extent to which the bank's businesses may be involved in the international movement of goods that could be used for terrorism or to finance terrorist activities. As such, the consideration and the extent to which terrorism or TF is occurring in jurisdictions with which the bank has close geographical and/or political links was monitored.
4. Vulnerabilities	i. The use and acceptance of cash in the system, although this is more focused on local resident clients or cash-generating local businesses. ii. The fast transactional nature of services across a range of currencies, including vulnerability to fraud against clients (money being taken from accounts). iii. Banks not understanding their own risks and vulnerabilities to ML/TF. iv. Business pressures, which could result from a group's strategy or approach, and may put commercial decisions ahead of regulatory concerns.

Factors	Isle of Man
5. Controls	i. Policies and procedures are in place to identify and verify all clients and TF risks, before onboarding. These policies and procedures include assessing the client risk through jurisdictional and industry risk exposure. ii. Clients are also sanctions-screened frequently. iii. Payment-screening is undertaken. iv. Trigger event processes are in place.

Table 39: Malawi foreign subsidiaries' TF risk understanding and controls

Factors	Malawi
1. Risk	The overall TF risk rating is low and the threat is primarily external.
2. Methodology	The subsidiary applies a risk-based approach in its risk management. This allows the bank to adopt a flexible set of measures to target its resources effectively and apply preventative measures commensurate with the nature of the risks. The same methodology is applied at head office level and at the subsidiary.
3. Threats	Malawi shares a border with Mozambique, which is known to have a growing number of human trafficking cases. There are branches close to the border that can be used for TF.
4. Vulnerabilities	i. Domestic threat: There are no known terrorist groups in Malawi targeting the country or other jurisdictions. ii. Regional threat: There are no known regional terrorist groups targeting Malawi. iii. Global threat: Islamic State (ISIS) and al-Qaeda are global groups with a regional presence. However, no known Malawian nationals are linked to the international terrorist groups. iv. Home jurisdiction used as a transit point: It is suspected that nationals from the region and elsewhere transit through Malawi en route to other countries.
5. Controls	Full know-your-client of all clients, including sanctions-screening and transaction-monitoring on all client accounts and ongoing due diligence.

Table 40: Zambia foreign subsidiaries' TF risk understanding and controls

Factors	Zambia
1. Risk	Medium to low (according to the national risk assessment for 2016).
2. Methodology	The subsidiary applies a risk-based approach in its risk management. This allows the bank to adopt a flexible set of measures to target the resources effectively and apply preventative measures commensurate with the nature of the risks. The same methodology is applied at head office level and at the subsidiary.
3. Threats	Zambia does not face any immediate TF risk but the volatile geopolitical situations in the Southern African Development Community, Great Lakes and East Africa regions could lead to the spread of terrorism and TF activities into the country. Zambia has had some foreigners from jurisdictions where there have been cases of terrorism whereby some of these foreign individuals may have sympathy for organisations involved in terrorist activities in their countries of origin.

Factors	Zambia
4. Vulnerabilities	Certain clients from jurisdictions with high terrorism activity may leave the entity vulnerable to TF. Some products that allow non-face-to-face interaction also increase TF risk. Clients such as embassies, NGOs and religious bodies also carry a high TF risk due to the source and destination of funds.
5. Controls	The subsidiary identified controls, some of which included the following: i. screening new and existing clients, employees, vendors/suppliers and related parties against sanctions lists; ii. payment-screening of cross-border transactions; iii. investigating and resolving potential matches generated during real-time and batch screening; and iv. screening and investigation of non-SWIFT cross-border payments (where required).

Table 41: eSwatini foreign subsidiaries' TF risk understanding and controls

Factors	eSwatini
1. Risk	The inherent TF risk rating is considered medium as recent developments in neighbouring countries, such as suspected terror al-Shabaab attacks in Mozambique, potentially increase the TF risk profile of eSwatini.
2. Methodology	A standardised approach is followed to identify and assess TF risks. The subsidiary has its own methodology customised in terms of its legislative requirements and aligned to the respective banking group standards.
3. Threats	i. Influx of foreign nationals from high-risk countries and the existence of the Hawala[28] system may potentially heighten TF risk in eSwatini. ii. An estimated 90% of the country's borders are shared with South Africa. To the east, the country shares a relatively small border with Mozambique. The small size and proximity of the country to the commercial cities of Maputo (Mozambique) and Johannesburg (South Africa) makes it attractive for cross-border illicit activities. iii. Recent developments in neighbouring countries, such as suspected terror attacks in South Africa and al-Shabaab attacks in Mozambique, potentially increase the TF risk profile of the country. iv. The current draft FATF mutual evaluation report also highlighted the abuse of credit cards outside the country, potential underground value transfers, extensive use of cash, porous borders, and potential abuse of money or value transfer services as potential threats.
4. Vulnerabilities	i. Potential funds-layering through credit card and debit card transactions, mostly in Asia, with unknown intended purposes that may include TF. ii. High usage of cash reduces the audit trail from source to expenditure

[28] Hawala is an informal method of transferring money without any physical money moving. It is described as a 'money transfer without money movement'.

Factors	eSwatini
	thereby increasing anonymity and potential abuse in relation to TF. iii. Legal persons and legal arrangements are inherently vulnerable to misuse for TF, because eSwatini does not have effective arrangements in place to register and maintain beneficial ownership information. iv. eSwatini has not identified NPOs that are likely to be at risk of TF abuse (due to their characteristics and activities) and, as a result, no measures have been implemented to identify the features and types of NPOs that may be vulnerable. v. Insufficient skilled human resources dedicated to financial investigations by competent authorities.
5. Controls	TF risk is identified through several mechanisms, including: i. specialised processes associated with trade finance; ii. client risk profiling, supported by a process for assigning a risk rating to jurisdictions, products and client types that involves assessing ML, TF and sanctions risk; and iii. transaction-monitoring system rules designed to detect a range of suspicious ML activities.

Table 42: Mauritius foreign subsidiaries' TF risk understanding and controls

Factors	Mauritius
1. Risk	A medium risk rating was allocated to the combination of ML and TF. They have not been rated separately.
2. Methodology	The subsidiary used the same approach and methodology as the group to conduct the TF risk assessment.
3. Threats	Due to the controls in place at the subsidiary, and in line with the compliance review conducted by independent consultants, the subsidiary concluded that no threats could be detected in relation to TF risk.
4. Vulnerabilities	Due to the controls in place at the subsidiary, and in line with the compliance review conducted by independent consultants, no threats could be detected in relation to TF risk.
5. Controls	Most controls were in place before the ML/TF risk assessment and are as follows: i. screening employees and vendors against relevant sanctions lists; ii. real-time screening of clients prior to onboarding; iii. daily screening of existing clients; iv. screening all cross-border SWIFT payments and all cross-border Common Monetary Area (CMA) EFT inward payments; and v. screening all trade finance transactions.

15.3 KnowYourCountry and terrorism financing

KnowYourCountry[29] is a global AML research tool used by financial institutions, regulators, government agencies and others. Table 43 summarises the findings related to TF and related activities in the listed countries.

The table below have been weighted based on findings focused on ML and sanctions issues. The ratings assigned are out of 100 and the higher the score, the more positive the rating in respect of a particular factor (e.g. 100/100 for international sanctions indicates that there are no international sanctions against a particular country).

Table 43: KnowYourCountry assessment findings[30]

Jurisdiction	International sanctions	Safe haven for or supporter of terrorism	TF-related risk concerns from KnowYourCountry reports as at 2019
Botswana	100/100	90/100	The US Department of State ML assessment found that: 1. Botswana is a cash-based society and has an insufficient framework for addressing ML and TF. 2. Botswana supplies many of the world's diamonds. The stringent institutional framework for the mining and processing of diamonds affords limited opportunity for organised diamond smuggling. The smuggling that does occur is not believed to be linked to TF or the laundering of criminal proceeds.
Ghana	100/100	90/100	1. The TF threat is generally moderate. Though the incidence of terrorism and TF in Ghana is low, the TF risk was rated high in the national risk assessment (NRA) due to Ghana's proximity to terrorism-prone countries, including Nigeria, Ivory Coast, Mali, Niger and Chad, and the emergence of ISIS and its social media campaign. 2. Ghana recently experienced a few cases of nationals joining ISIS as foreign terrorist fighters.

[29] KnowYourCountry: global anti-money laundering esearch Tool – available at https://www.knowyourcountry.com/
[30] KnowYourCountry: global anti-money laundering research tool – available at https://www.knowyourcountry.com/

Jurisdiction	International sanctions	Safe haven for or supporter of terrorism	TF-related risk concerns from KnowYourCountry reports as at 2019
			3. Ghana has developed a national counter-terrorism strategy; however, the strategy does not directly address TF.
Isle of Man	100/100	90/100	1. There is no local dedicated anti-terrorism unit although training has been provided to some police officers. 2. The TF threat assessment appears to be missing an important element: an assessment of the flows leaving the jurisdiction, which could potentially be linked to TF, terrorist groups or individual terrorists in other countries, especially in high-risk jurisdictions. 3. In 2015, the government of the Isle of Man amended the Proceeds of Crime Act 2008, so that it covers bitcoin companies, such as exchanges, operating from the island. 4. The lack of data related to outward and incoming flows of funds and the beneficial owners of assets managed or funds held in the jurisdiction creates challenges in determining whether any flows leaving the jurisdiction could be linked to TF, terrorist groups or individual terrorists in other countries, especially in high-risk jurisdictions.
Mozambique	100/100	90/100	1. ML in Mozambique is driven by misappropriation of state funds, kidnappings, human trafficking, narcotics trafficking, wildlife trafficking and terrorism. 2. Due to its largely unpatrolled coastline, porous land borders and limited rural law enforcement presence, Mozambique is a major corridor for illicit goods, including hardwoods, gemstones, wildlife products and narcotics. 3. Mozambique experienced a significant increase in terrorist activity in 2019. ISIS's affiliate in Mozambique carried out numerous attacks in northern Mozambique and Tanzania, resulting in the estimated deaths of 350 civilians and the internal displacement of 100 000 people. 4. The government of Mozambique continued security operations against the ISIS-affiliated group in 2019 and arrested numerous terrorist suspects. In June 2019, ISIS began claiming responsibility for the attacks. 5. From September to November 2019, Russia provided operational support for the government-led counter-terrorism operations. 6. ISIS attacks in this area threatened employees of an international liquid natural gas consortium, in which a US company is a participant, prompting

Jurisdiction	International sanctions	Safe haven for or supporter of terrorism	TF-related risk concerns from KnowYourCountry reports as at 2019
			the consortium to approach further investment in Mozambique with caution. 7. ISIS's affiliate in Mozambique reportedly conducted weekly or more frequent attacks on rural villages in Mozambique's northern Cabo Delgado province. Fighters connected to this affiliate are frequently reported to wear stolen police or military uniforms. 8. Border security remains a significant security challenge for Mozambique. Terrorists are known to cross the porous border into and from Tanzania, which serves as a recruitment and transit point for terrorist and criminal organisations.
eSwatini	100/100	90/100	1. The Kingdom of eSwatini started implementing AML measures in 2001 and anti-TF measures in 2008. These measures remain at infancy stage, owing mainly to inadequate structures and resources to drive the process. 2. Some traders transact in cash only and not through banks. Human trafficking is widespread. 3. eSwatini officials believe the Kingdom to be at low risk for TF.
United Kingdom	100/100	90/100	1. The UK faces severe threats from international terrorism. 2. TF activity in the UK is usually low-level, involving small amounts of funds raised by UK-based individuals for their travel to join terrorist groups, to send to terrorist associates, or to finance their own terrorist attack plans. 3. The UK also faces threats from Northern Ireland-related terrorism which are rated severe in Northern Ireland and substantial in Great Britain. The nature of this threat has evolved, with paramilitary and terrorist groups focusing on various forms of organised crime, not all of which specifically intend to raise funds for terrorism. 4. Particularly good results are being achieved in investigating and prosecuting ML/TF cases, confiscation, implementing targeted financial sanctions related to terrorism and proliferation, protecting the non-profit sector from terrorist abuse, understanding the ML/TF risks facing the country, preventing misuse of legal structures, and cooperating domestically and internationally to address them. 5. Through most of 2019, the terrorism threat level in the UK was at the second-highest rating (severe).

Jurisdiction	International sanctions	Safe haven for or supporter of terrorism	TF-related risk concerns from KnowYourCountry reports as at 2019
			6. In early November 2019, the UK lowered the threat level to substantial, meaning the threat of an attack was reduced from 'highly likely' to 'likely'. 7. UK officials categorise Islamist terrorism as the greatest threat to national security, though officials identify a rising threat, which they refer to as 'extreme right-wing' terrorism. 8. The threat level for Northern Ireland-related terrorism within Northern Ireland, set separately from England, Scotland and Wales, remains severe. 9. According to UK Home Office figures, UK law enforcement agencies made 266 arrests for terrorism-related activity from January to June 2019. As a result, 63 individuals were charged with terrorism-related offenses. The Metropolitan Police report about 800 active investigations involving about 3 000 individuals. 10. For the 2018/2019 period, the UK convicted 50 people of terrorism-related offenses and currently has more than 200 people in custody. Of those convicted, 76% received sentences of less than 10 years. Three were sentenced to life in prison.
Zambia	100/100	90/100	1. The risks of terrorism and TF are well understood by the Zambian authorities. 2. The authorities are of the view that the threat of TF or terrorism does not arise from locals but from some foreign nationals from high-risk TF countries. 3. Zambia remains vulnerable to these threats because it is predominantly a cash economy, therefore most of the transactions are undocumented or processed through informal transmission mechanisms such as hawala; it has long porous land borders that could be abused by terrorists or terrorist financiers; and it is a transit country, with a high volume of people entering and leaving the country. 4. Volatility is caused by the militant group al-Shabaab in East Africa and the Horn of Africa. 5. Inadequate resources and training impeded Zambia's law enforcement agencies' counter-terrorism capabilities. 6. Zambia's long and porous borders continued to pose a challenge in terms of the monitoring and control of illegal immigrants attempting to enter the country. 7. Zambia is vulnerable to human trafficking and

Jurisdiction	International sanctions	Safe haven for or supporter of terrorism	TF-related risk concerns from KnowYourCountry reports as at 2019
			international crime.
Zimbabwe	33.3/100	90/100	1. The authorities demonstrated good national cooperation and coordination when they successfully investigated a suspected TF case, using financial intelligence to identify the movements of funds involved. 2. There has been no outreach to the NPO sector and the regulator has not yet identified NPOs that pose high TF risk with a view to apply proportionate controls. 3. According to the national risk assessment (NRA) concluded, the risk of TF in the country is low considering a number of factors, including risk level in the region, understanding of TF threats and risks by relevant competent authorities and financial institutions, and the absence of known TF or terrorism cases in the country. 4. Zimbabwean law enforcement officials have been reluctant to take or recommend actions that would be seen as pro-American. 5. Zimbabwe's framework to freeze terrorist assets has yet to be proven effective.

15.4 Evolution of terrorist threats within Kenya, Nigeria, Uganda and the Democratic Republic of Congo

15.4.1 Terrorism statistics

The data behind Figures 17 to 20 depicts growing terrorism activities in African countries with Islamist extremism and/or governments unable to provide fiscal stimulus.[31] The rise of civil unrest at a sub-national level, resource scarcity, geographical change, territorial disputes and political dysfunction contribute to the increase in existing group rivalries and/or creating new ones.

[31] Aon in partnership with the Risk Advisory Group and Continuum Economics. Risk maps 2020. Available at https://www.aon.com/getmedia/14163391-65f2-4fc0-95a5-c130a0a63f15/Aon-Risk-Maps-2020.aspx

Figure 17: Number of terrorism-related deaths in African countries from 2007 to 2019[32]

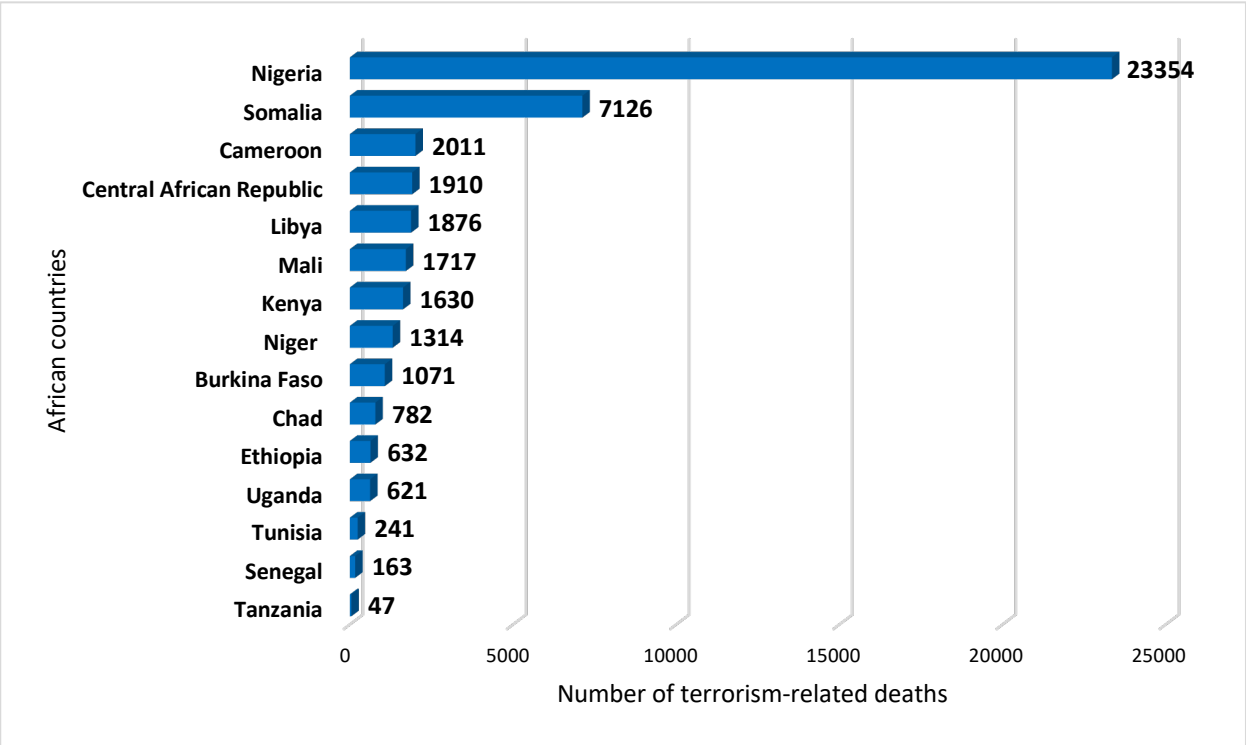
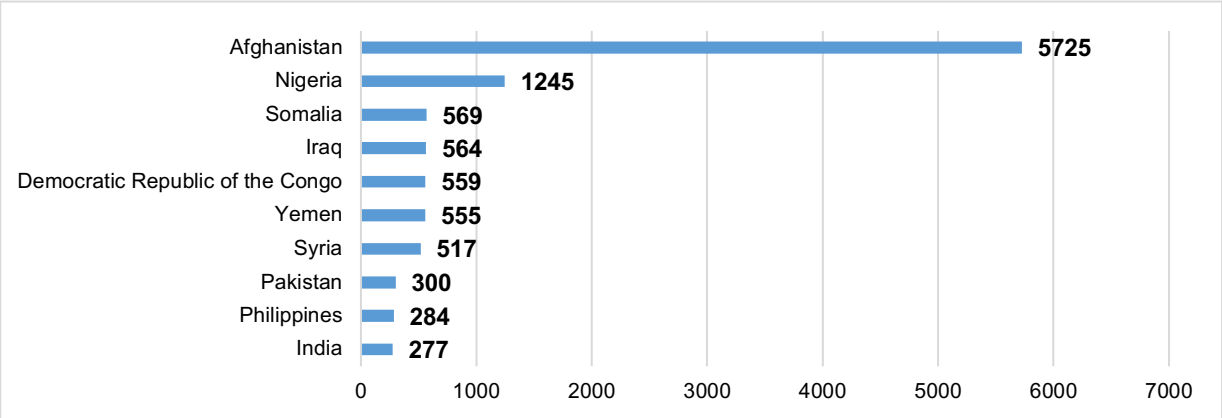


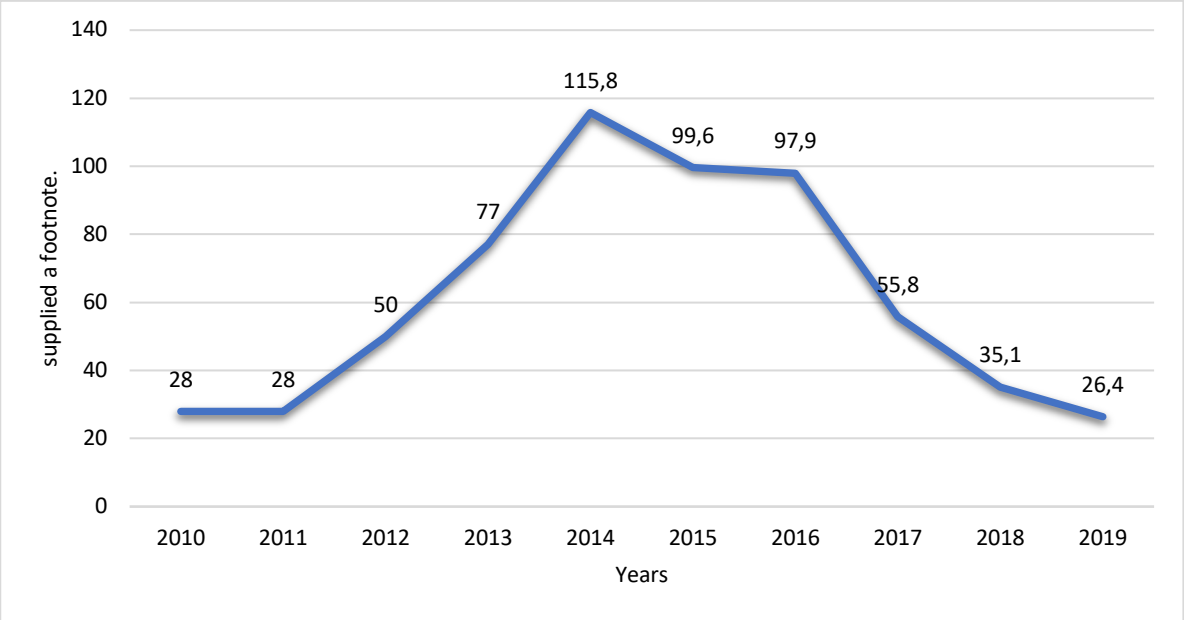
Figure 18: Number of deaths in countries most affected by terrorism in 2019[33]



[32] Statista. November 2020. Available at https://www.statista.com/statistics/1197884/number-of-deaths-from-terrorism-in-africa-by-country/

[33] Statista. 2019. *Number of deaths in the countries most impacted by terrorism in 2019.* Available at https://www.statista.com/statistics/377070/countries-most-impacted-by-terrorism-number-of-deaths/

Figure 19: Global economic cost of terrorism from 2010 to 2019[34]



Aon's Terrorism and Political Violence map[35] for the first quarter of 2021 highlighted the countries listed below as very high risk for deterioration linked to the following core risk measures: country, legal and regulatory (for example, financial or reputational as a result of compliance deficiencies), political violence (for example, riots, strikes and civic commotions), and risk of doing business:

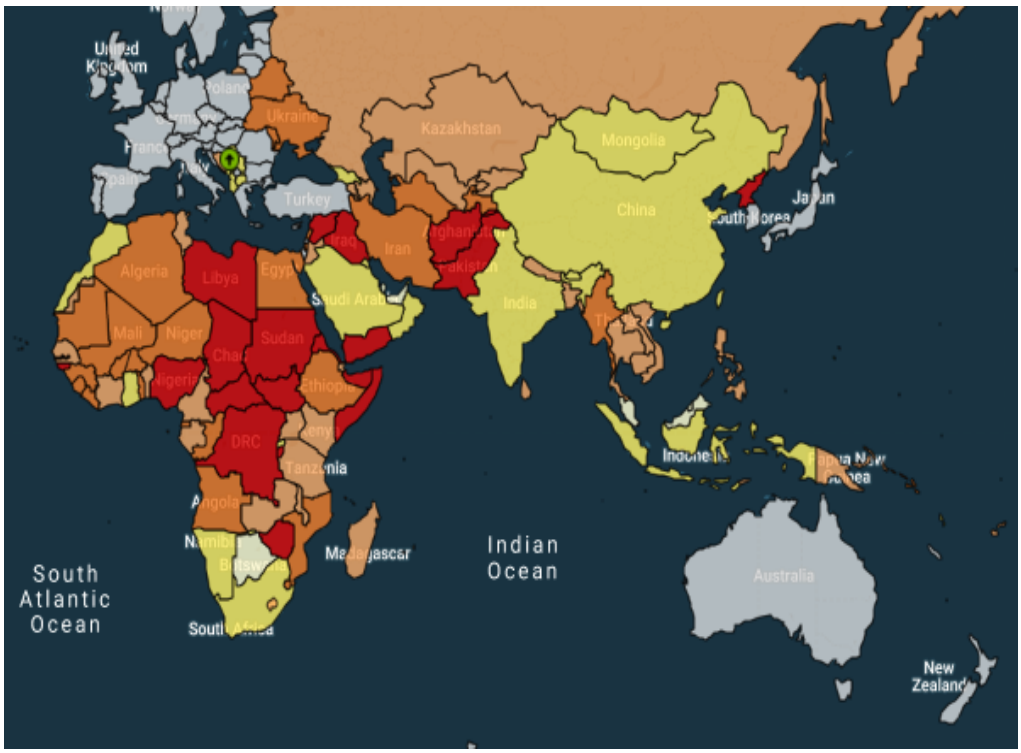
- Mozambique
- Democratic Republic of Congo
- Nigeria
- Sudan
- Chad
- Libya
- Iraq

[34] Statista. 2020. *Global economic cost of terrorism 2000 to 2019*. Available at https://www.statista.com/statistics/489649/global-economic-costs-of-terrorism/

[35] Aon Empower. 2021. *Heat Map – Political Risk Map*. Available at Aon Risk Portal – Risk Map 2022 available at: https://www.aon.com/2020-political-risk-terrorism-and-political-violence-maps/index.html

- Afghanistan
- Pakistan

Figure 20: Aon's latest Terrorism and Political Violence map[36]



As at 31 October 2021, South African banks operated 52 cross-border banking operations in 25 jurisdictions on 3 continents. From the FATF Mutual Evaluation 4th round ratings for TF, the PA observed that:

- 13 out of the 25 (52%) jurisdictions had been subjected to a FATF mutual evaluation;
- 10 out of the 13 (77%) jurisdictions were rated as having a low effectiveness[37];
- 2 out of the 13 (15%) jurisdictions were rated as having a moderate effectiveness;

[36] Anon Empower Results 2021 Heat Map – Political Risk Map Available at: Aon Risk Portal- Risk Map 2022.
[37] The Immediate Outcome is not achieved or achieved to a negligible extent. Fundamental improvements needed.

- 1 out of 13 (8%) jurisdictions was rated as having a high effectiveness for FATF Immediate Outcome (IO) 9 (TF investigation and prosecution), IO 10 (TF preventive measures and financial sanctions) and IO 11 (PF financial sanctions); and
- the majority of African countries assessed received a low effectiveness rating across IOs 9, 10 and 11.

15.4.2 Methods and typologies for financing domestic extreme right-wing organisations

Extremism is not localised. According to a UN Office on Drugs and Crime article on the subject, violent extremism is characterised by marginalisation, lack of opportunities and grievances with the state. This creates an ideal opportunity for terrorist groups to exploit and recruit more socio-economically vulnerable individuals.[38]

The following financing methods were identified for domestic extreme right-wing organisations:

- **self-funding**, using own assets and access to personal and retail credit lines;
- crowdfunding, through the use of social media targeting the wider community or a designated closed group;
- **crypto assets**, as some groups created their own cryptocurrency to transact between members and raise funds;
- **alternative payment systems**, such as companies specialising in debit order collections that were identified as facilitating monthly membership contributions for extreme right-wing groups;
- **donations**, or generating funds through cash deposits and electronic transfers referenced as donations;

[38] United Nations Office on Drugs and Crime. *Preventing Violent Extremism Conducive to Terrorism*. Available at https://www.unodc.org/unodc/en/terrorism/expertise/preventing-violent-extremism-conducive-to-terrorism.html

- **specialised training**, as these groups offered members and specific communities training, including self-defence, personal protection and anti-hijacking training, and training to prevent farm attacks and house robberies;
- **international fund transfers**, indicating that some of the organisations receive financial support from individuals – who appear to be South African nationals, per the transactional references – in foreign jurisdictions. These jurisdictions include the US, United Arab Emirates, Australia and Switzerland; and
- **NPOs**, as some extreme right-wing organisations are registered as NPOs and their representatives travel to other countries such as the USA and Canada to lobby for support and raise funds.

Through analysis provided by the FIC, it was established that domestic extreme right-wing organisations may set themselves up to facilitate financing through the following:

1. registering the organisation as a non-profit entity; and
2. opening bank accounts in the name of the registered entity and having the leadership of the organisations use their personal bank accounts to collect funds on behalf of the organisation.

The FIC released the TF National Risk Assessment (TF NRA) in 2022[39] which highlighted the following terrorism financing vulnerabilities in South Africa:

- cash and alternative remittance services;
- border integrity;
- charities and NPOs;
- support for ISIS in South Africa;
- foreign terrorist fighters;

[39]The 2022 South African Terrorism Financing National Risk Assessment (TF NRA). Available at https://www.fic.gov.za/Documents/TF%20NRA%2031%20March%202022.pdf

- terrorism financing and organised crime nexus; and
- virtual currencies.

The TF NRA highlighted the following:

South Africa has several domestic terrorism and terrorism financing risk factors to consider. Support for Foreign Terrorist Organisations (FTOs) in the form of South African nationals who have travelled to and returned from conflict zones as well as foreign suspected terrorists transiting through or staying in South Africa is acknowledged. South Africa has a history of isolated incidents of domestic extremism, particularly violent right-wing extremism, that is continuously monitored but is not currently deemed to be as high a risk as international terrorism trends and terrorist groups.

15.5 Banking sector's inherent TF risk category

Table 44: TF risk category

Large banks	Locally controlled banks	Branches of foreign banks and foreign controlled banks	Mutual banks
High	High	High	High

Overall risk: High

The rationale for the above rating is as follows:

- The banking sector is exposed to possible terrorism and TF risks due to a lack of understanding of TF vulnerabilities and how terrorist financiers operate, which channels are preferable, and how the sector and/or a bank could be subject to abuse.
- Sanctions-screening may take place but may only address persons listed on specific UN lists, excluding potential domestic TF threats that may exist.
- There has been a significant increase in terror-related activities and TF within jurisdictions where South African banks have a presence through subsidiary banks, for example Mozambique, Kenya and Nigeria.

- South Africa's proximity to terrorism-prone countries such as Mozambique, Nigeria, Kenya and the Democratic Republic of Congo could potentially increase the terrorism risk and TF risk for South African banks.
- Cash-based products and/or services delivered by banks provide an insufficient framework for addressing TF.
- Innovative new payment systems (such as cryptocurrency and prepaid cards) create opportunities for terrorists to access finance.
- Terrorists constantly adapt how and where they move their funds to circumvent safeguards that countries have put in place.
- Concerns stemming from the FATF/FATF-styled regional body mutual evaluations of the relevant countries were observed with regard to the TF risk.

16. Reporting obligations

16.1 Cash threshold reporting

16.1.1 Introduction

Section 28 of the FIC Act places an obligation on AIss to report cash threshold transactions and aggregated cash transactions above the value of R24 999.99 to the FIC within two business days.

16.1.2 Analysis of cash threshold data from the banks

All 34 banks were requested to provide the statistics of CTRs and cash threshold report aggregations (CTRAs) filed with the FIC for the period 1 October 2018 to 31 December 2020. Based on the information received from the banking sector, a total of 3 705 251 CTRs and 6 233 924 CTRAs were identified and reported during the period. The graphs below show the percentages of CTRs and CTRAs reported by the banking subsectors.

Figure 21: Percentages of CTRs reported by all banks

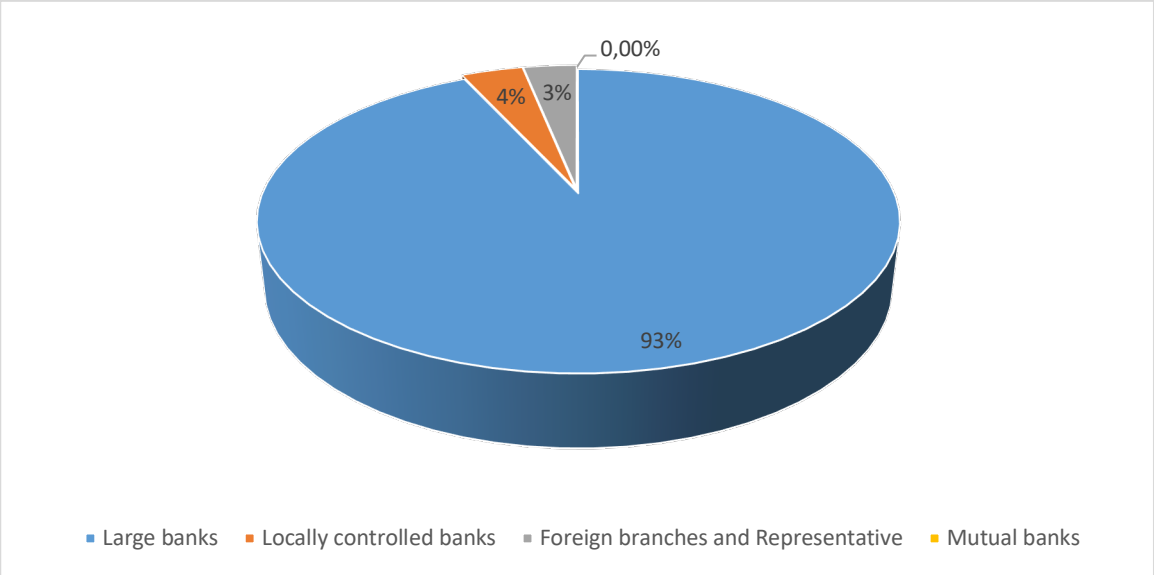
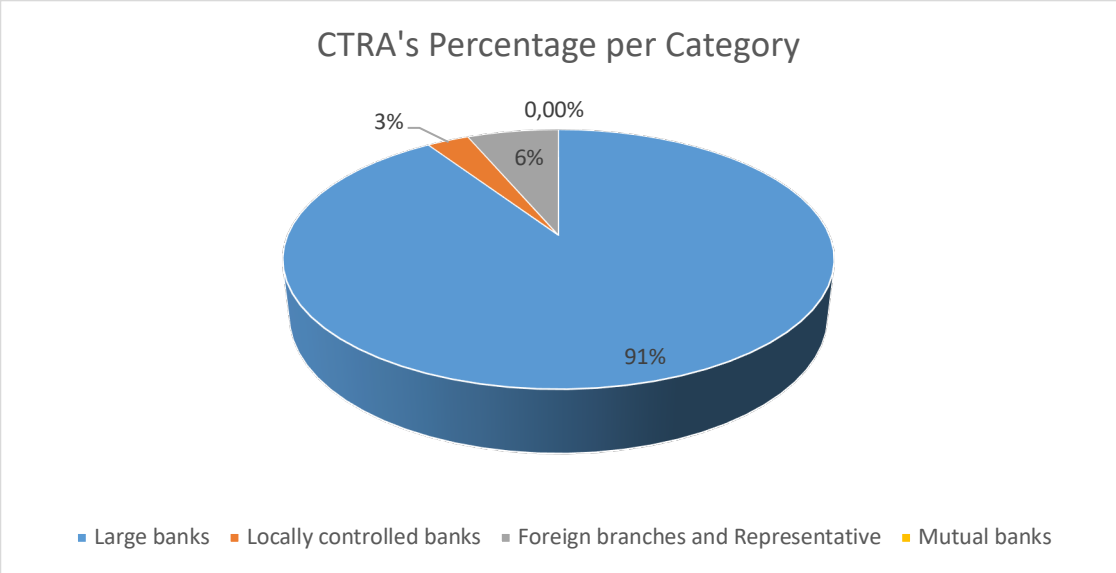


Figure 22: Percentages of CTRAs reported by all banks



The majority of the CTRs and CTRAs were reported by the five large banks. Mutual banks had the lowest number of CTRs and the digital mutual bank reported no CTRs or CTRAs.

Furthermore, the information was averaged to determine average CTRs and CTRAs reported monthly and quarterly per category as detailed below. The large banks had the largest averages, and the mutual banks had the lowest averages. The monthly and quarterly averages of the locally controlled banks and the branches of foreign banks and subsidiaries were within the same ranges.

Table 45 and Table 46: Averages of CTRs/CTRAs per categories of banks

Category of bank	Total average CTRs	Monthly average CTRs	Quarterly average CTRs
Large banks	689 914	25 552	76 657
Locally controlled banks	17 186	637	1 910
Branches of foreign banks and subsidiaries	11 810	437	1 312
Mutual banks	47	2	5

Category of bank	Total average CTRAs	Monthly average CTRAs	Quarterly average CTRAs
Large banks	1 130 105	41 856	125 567
Locally controlled banks	23 019	853	2 558
Branches of foreign banks and subsidiaries	39 922	1 479	4 436
Mutual banks	9	0	1

16.2 Cash threshold reporting data from the FIC

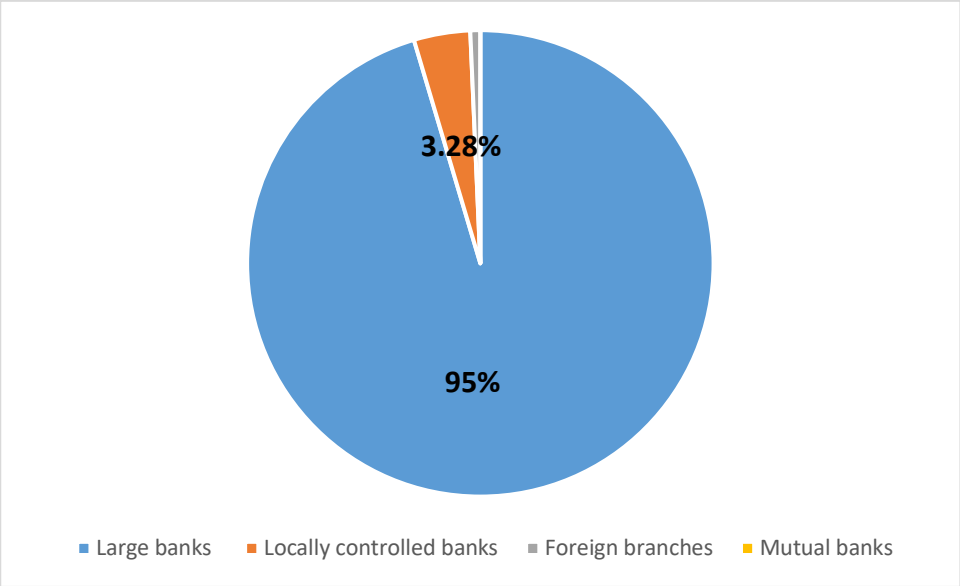
The FIC provided the statistical information of CTRs, CTRAs, remediated cash threshold reports and remediated cash threshold reports aggregated. This information was submitted by the banking sector for the period 1 October 2018 to 30 September 2020.[40] The FIC disclosed that, at the time of the submission, the figures submitted to the PA were not audited.

16.2.1 Analysis of cash threshold reporting data

The FIC received a total of 9 294 823 section 28 reports with a total value amounting to approximately R14 billion for the period. The number of section 28 reports were recorded as shown in the following graph.

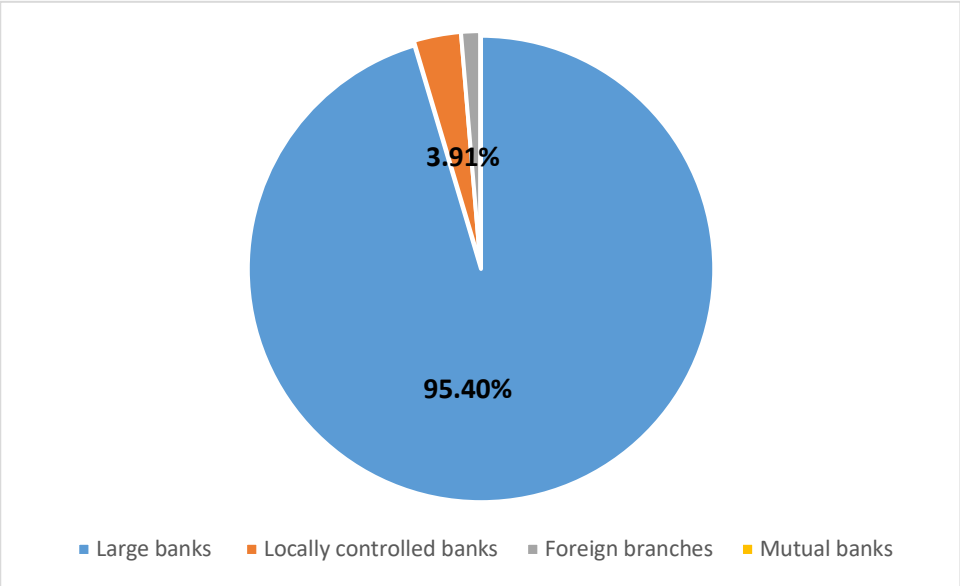
[40] The information submitted by the FIC excluded the three licensed mutual banks, as no data was submitted for these banks.

Figure 23: Total CTRs reported by the banking sector



The large banks submitted most of the section 28 reports, followed by the locally controlled banks at 3.28%. The foreign branches or subsidiaries submitted the remaining 0.69% of these reports.

Figure 24: Total CTRAs reported by the banking sector



The large banks dominated the submission of CTRAs, followed by the locally controlled banks.

Table 47: Total number of CTRs and CTRAs

Category of bank	Number of CTRs submitted	Percentage of all CTRs	Number of CTRAs submitted	Percentage of all CTRAs
Large banks	2 431 808	95.39%	5 154 453	95.40%
Locally controlled banks	83 539	3.28%	211 123	3.91%
Branches of foreign banks or subsidiaries	33 873	1.33%	37 335	0.69%
Total	**2 549 220**	**100**	**5 402 911**	**100**

The FIC also provided information where the banking sector had to remediate the reports filed due to issues in the banks. Table 48 shows the number of reports that were remediated for the reviewed period.

Table 48: Number of remediated section 28 reports

Category of bank	Number of remediated CTRs submitted	Number of remediated CTRAs submitted
Large banks	2 697	1 337 230
Locally controlled banks	9	2 756
Branches of foreign banks or subsidiaries	0	0
Total	**2 706**	**1 339 986**

Two of the five large banks submitted most of the remediated reports, with one large bank contributing 82% of all submissions. The locally controlled banks followed, with only one bank submitting remediated reports.

The FIC has a process for banks to provide notification of failure to report as required by the FIC Act. The FIC issued Directive 03/2014, which allows the banks to engage the FIC on any reporting failures. It also provided information on banks that notified the FIC in terms of this directive. Missing information, such as the client's identity number or passport, and incorrect or non-completion of the required information were the most common causes of these rejections. The banks submitted the following failures to the FIC.

The FIC's general comments in terms of Directive 03/2014 outcomes were as follows:

- Bank reporters do not submit all the CTR/CTRA reports due to the FIC because of not ensuring that all their product and services lines are included when programming or reviewing their automatic transaction monitoring systems.
- There is a lack of oversight from a multi-disciplinary monitoring team within banks, including information and communications technology (ICT) and compliance officers and compliance teams, because issues are picked up long after they have occurred.
- In terms of quality, bank reporters do not seem to have all the basic required information readily available for reporting to the FIC in terms of the regulations. This points to a continued failure to adhere to broad and specific CDD and EDD requirements.

16.2.2 CTR and CTRA typologies and/or anomalies noted in the data

The FIC analysed the CTRs for the 2020/2021 financial year. It completed analysis for April 2020, May 2020 and June 2020 where the FIC provided data. During this period, South Africa was in lockdown due to COVID-19, which, according to the FIC, also affected the transactional behaviour of clients. The banks reported the highest reportable cash transactions.

The FIC reported that most cash transactions were of individuals depositing cash above the threshold into their accounts, and entities withdrawing cash above the prescribed threshold. Various unusual cash transactions were identified and referred for further analysis and potential referral to law enforcement agencies. The main suspicious indicators identified were:

- potential corruption linked to tenders;
- large cash transactions used by influential political persons (local and domestic);
- individuals using their personal accounts for business purposes (potential tax evasion);
- large and complex structures used to move funds between companies;

- businesses prohibited from trading under lockdown regulations were still moving money;
- NPO transactions identified as potential TF/PF activities;
- potential fronting, where the value of cash transactions paid and received by the company is not in proportion to the products and/or services the company purports to deal in; and
- various indicators showing that money mules are used to move cash out of the country, in particular to Middle Eastern countries, where the source of funds could not be determined.

The predominant anomalies identified through the analysis were:

- the quality of location-based data in the CTR dataset was in many instances very poor;
- a large percentage (78%) of depositors' information was not available or not captured when individuals deposit money into an account;
- one of the large banks may have reported EFTs as cash transactions, causing the CTR figures to be inflated;
- potentially incorrect reporting scenarios by banks (and other AIs/reporting institutions were identified, such as person-to-person transactions (AIs only involved in certain money remittance scenarios), or account-to-account transactions (EFTs only reportable as cash transactions in agency banking scenarios).

The use of cash in the banking sector presents a ML/TF risk as many banks offer products used to obtain cash, and the audit trail is diminished once the proceeds of crime are converted into cash and withdrawn. Mule accounts are also created to enable the proceeds of crime to be withdrawn as cash and create a second layer of anonymity between the criminal and these proceeds.

Deposits can be made by both clients and non-clients into the accounts of banked clients, and the degree of due diligence obtained in respect of the depositor affects the bank's ability to assess the risk associated with this transaction. The funds could be a donation, a payment from a stranger not linked to any legitimate

purpose, the proceeds of crime from corrupt activities being deposited into mule accounts, or something else.

Some cash products offered by banks allow a person to make a cash payment to a non-client relatively easily, using a cellphone to validate payments and provide a code to the non-client who can then obtain the money. A large bank that offered this product saw payments totalling billions of rands being transferred and withdrawn as cash. The anonymity with this product is also a potential avenue for criminal abuse.

17. Suspicious and unusual transaction reporting

17.1 Analysis of data received from banks

Section 29 of the FIC Act places an obligation on AIs to file suspicious transaction reports (STRs) and suspicious activity reports (SARs) with the FIC. All banks in South Africa must file a transaction or an activity if they have reasonable grounds to suspect that they have received the proceeds of a criminal offence or seen activities related to a criminal offence.

Over the period 1 October 2018 to 28 December 2020, information provided by banks indicated that a total of 2 020 176 automated STR alerts were generated, of which 506 936 were filed with the FIC.

Furthermore, 541 508 manual alerts were generated and investigated by the banks, of which 165 531 resulted in the submission of STRs to the FIC. Out of 530 442 SAR alerts generated and investigated, 75 810 resulted in reports being submitted to the FIC. The number of reports is outlined by banking subsectors in the following graphs.

Figure 25: Suspicious and unusual reporting by large banks

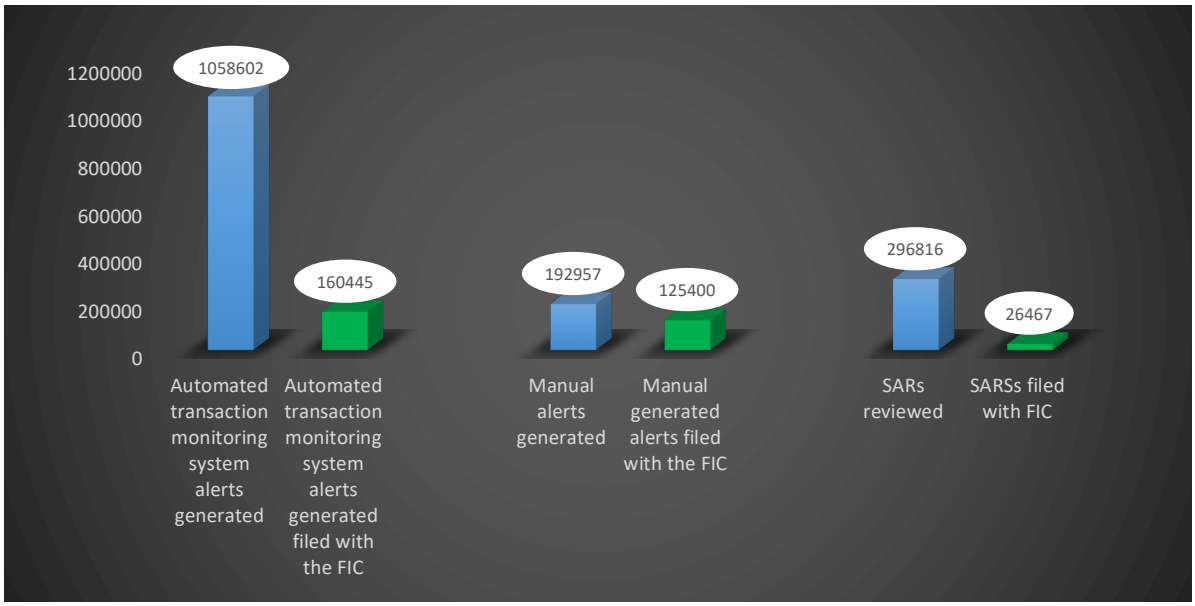


Figure 26: Suspicious and unusual reporting by locally controlled banks

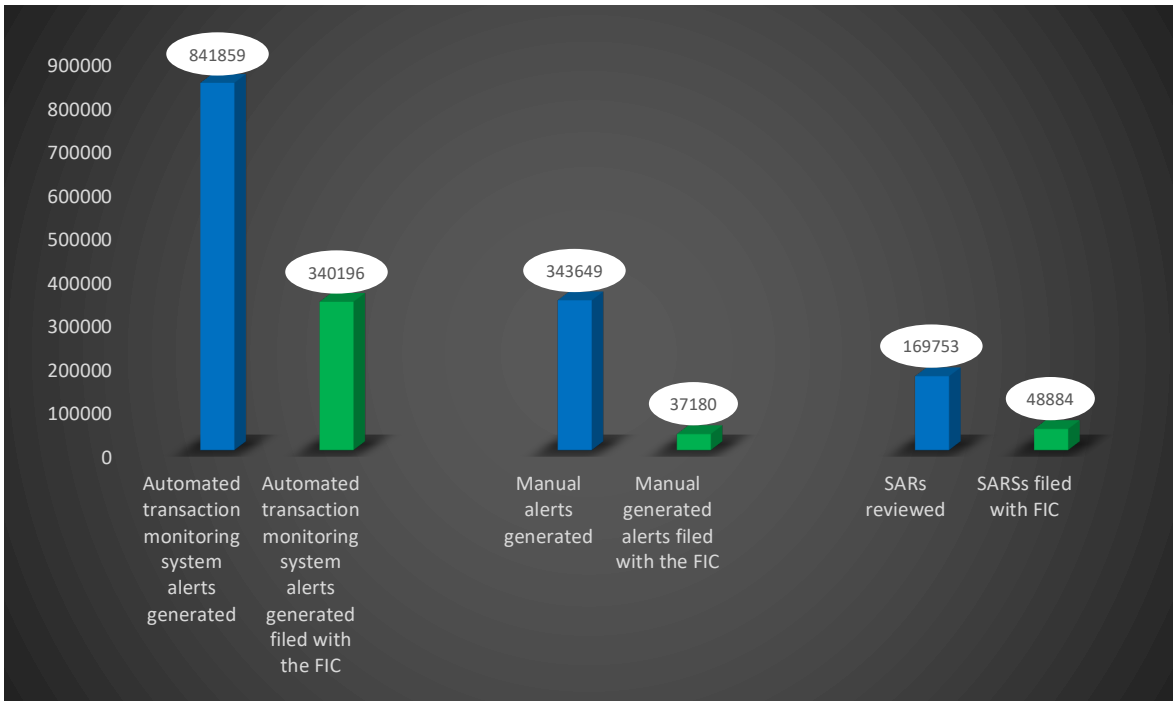


Figure 27: Suspicious and unusual reporting by branches of foreign banks and foreign controlled banks

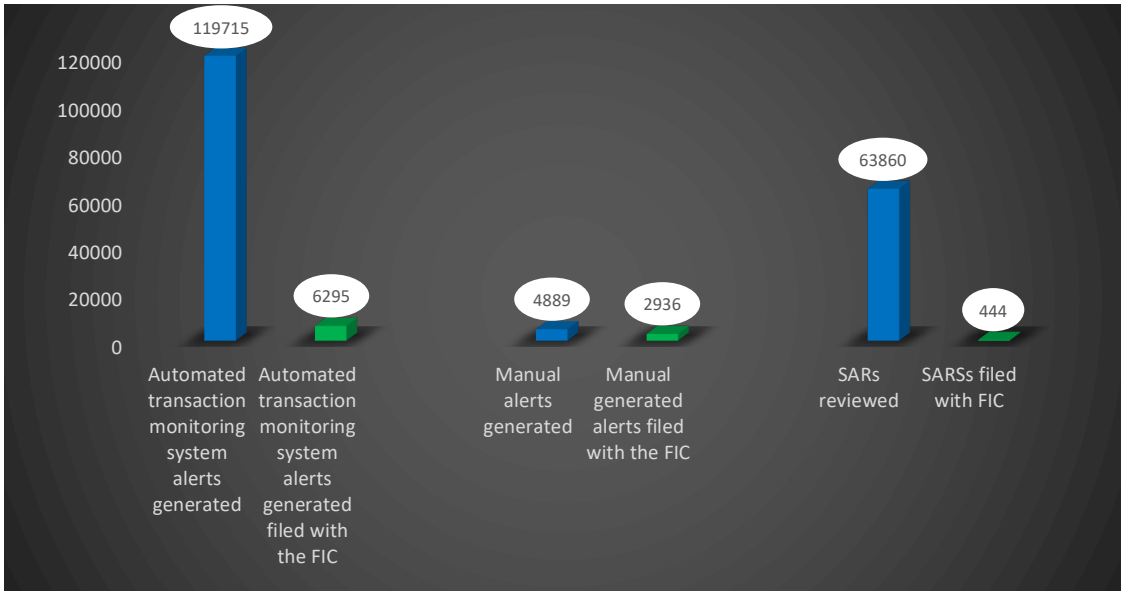
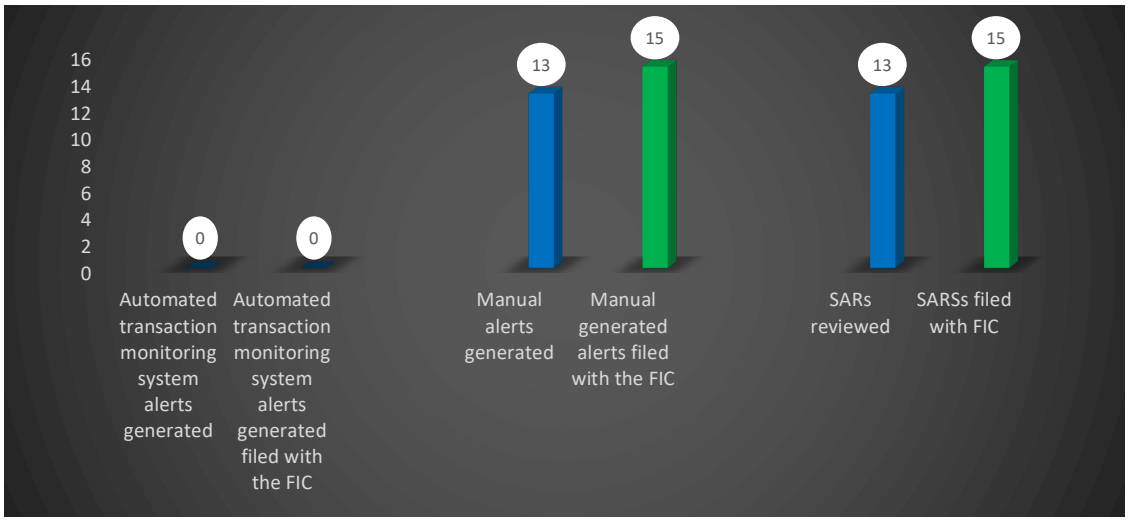


Figure 28: Suspicious and unusual reporting by mutual banks



Furthermore, 38 105 suspicious transaction or activity reports were linked to high-risk clients, and 602 505 CTRs/CTRAs – of which 252 793 were linked to high-risk clients – were converted to STRs.

Table 49: Reports linked to high-risk clients and conversion of reports

Category of banks	Number of STRs/SARs linked to high-risk clients	Percentage	Number of CTRs/ CTRAs converted to STRs	Percentage	Number of CTRs/ CTRAs converted to STRs linked to high-risk clients	Percentage
Large banks	30 413	79.81%	126 807	21.05%	58 086	22.98%
Locally controlled banks	7 594	19.93%	475 625	78.94%	194 703	77.02%
Branches of foreign banks or subsidiaries	97	0.25%	72	0.012	4	0.002%
Mutual banks	1	0.003%	1	0.0002	0	0%
Total	38 105	100%	602 505	100%	252 793	100%

The common predicate offences often identified through the reporting process for the 31 banks – all banks excluding the three mutual banks which did not identify any predicate offences – included:

- corruption;
- bribery;
- ML;
- tax evasion;
- fraud;
- internet and related scams;
- drug trafficking;
- cryptocurrency-related transactions; and
- illegal wildlife trade and pyramid schemes.

The following trends and typologies were identified:

- Tax evasion – most clients open personal accounts but use them for business purposes. This is picked up through a client's transactional activity and is usually followed by queries from law enforcement and tax revenue authorities.

Other triggers include structuring of cash deposits followed by large withdrawals.

- Fraud identified through the STR portal, with alerts pertaining to scams and subpoenas.
- Cross-border movements – cash received into accounts and immediately transferred outward. Multiple money service provider payments received from various sources.
- Pyramid and Ponzi schemes – transactions appeared to be part of a pyramid scheme in that many transactions from different individuals involve particular account holders.
- Forgery and scamming – clients provided fictitious CDD documentation (e.g. fake ID documents/bank statements).
- Credit card application fraud (South African Banking Risk and Information Centre) linked to COVID-19 credit relief programmes.
- Wildlife trafficking – a high number of inquiries were received through subpoenas related to clients involved in wildlife trafficking.
- Advance payments – companies used advance payments to externalise funds without any goods received in South Africa.
- Deviation from onboarding agreement – transacting patterns did not match client information provided at onboarding.
- Trends relating to high-volume cash deposits, coupled with rapid use of funds, for both businesses and individuals (often Chinese nationals).
- Fraudulent South African Revenue Service (SARS) payments were received and then rapidly disposed of.[41]
- South African mules, newly opened accounts, self-employed or unemployed people making a once-off foreign investment.

[41] Potential corrupt individuals involved or fraudsters exploiting SARs for gain.

- Loan agreements without an interest rate, no clear owner of asset and no clear rule around profit or loss when things go wrong.
- Large cash deposits, out of line with the profile of the client.
- Prostitution, and human and drug trafficking.
- Armed robbery.

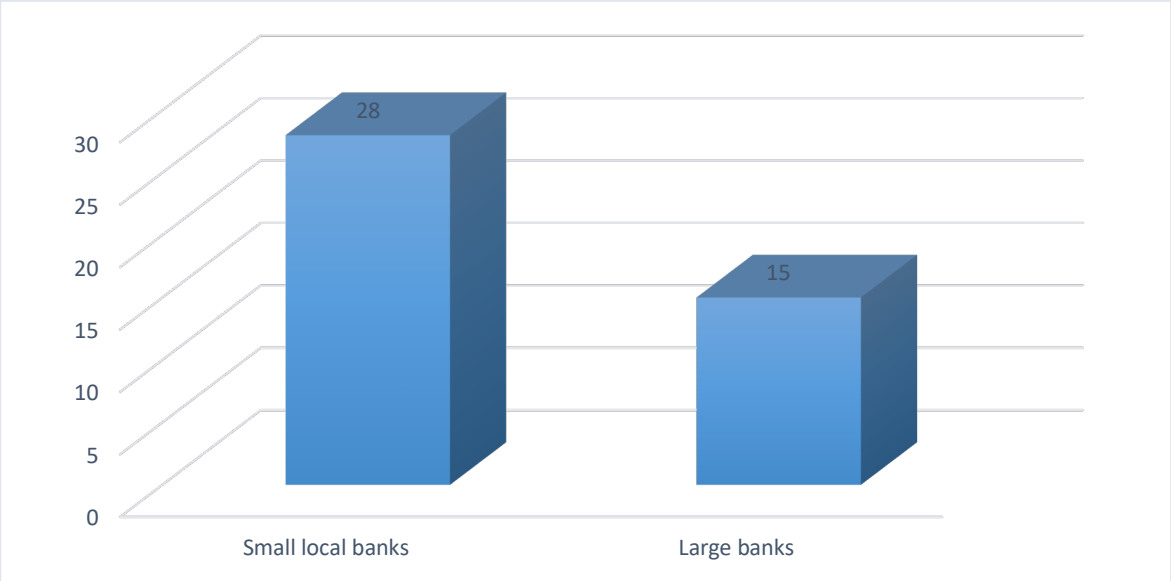
The most common issues reported in the STRs that point to possible ML risk were:

- corruption;
- unusual cash activity;
- Ponzi schemes;
- illicit cross-border flows;
- capital flight – excessive funds sent out of the country by foreign nationals;
- fraud;
- tax evasion;
- racketeering;
- drug trafficking;
- internet scams; and
- advance fee scams.

17.2 Terrorist financing transaction or activity reports reported to the FIC

The banking sector reported 43 terrorist financing activity reports (TFARs) and 9 terrorist financing transaction reports (TFTRs) to the FIC in terms of section 29(1)(a), (c) or 29(2) of the FIC Act for the period 1 October 2018 to 31 December 2021. All nine TFTRs were reported by large banks. The graph below illustrates the TFARs and TFTRs reported by locally owned banks and large banks.

Figure 29: TFARs and TFTRs reported to the FIC



17.3 Analysis of section 29 reports provided by the FIC

17.3.1 Statistics of section 29 reports

The FIC provided the statistics of STRs, SARs, TFTRs, TFARs and STRs reported in batches submitted by the banks and the number submitted by the banking sector.[42] Below is a breakdown of the section 29 reports processed by the FIC for the period 1 October 2018 to 31 December 2020.

Table 50: Number of section 29 reports filed by all banks

Category of banks	Suspicious transaction reports (STRs)	Suspicious activity reports (SARs)	TF transaction reports	TF activity reports	STRs reported in batches	Total
Large banks	270 522	42 925	27	45	3 608	317 127
Locally controlled banks	273 195	42 994	28	45	3 644	319 906

[42] No suspicious transaction or activity report statistics were provided for the mutual banks

Branches of foreign banks or foreign controlled banks	7 937	635	0	1	0	8 573
Total	551 654	86 554	55	91	7 252	645 606

Figure 30: Number of section 29 reports by all banks

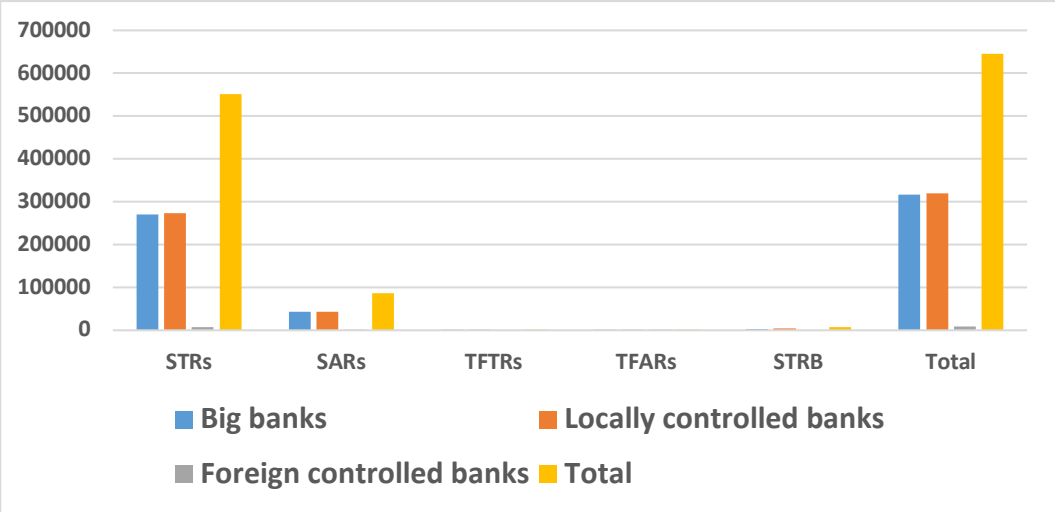


Figure 31: Number of section 29 reports processed by the FIC per year

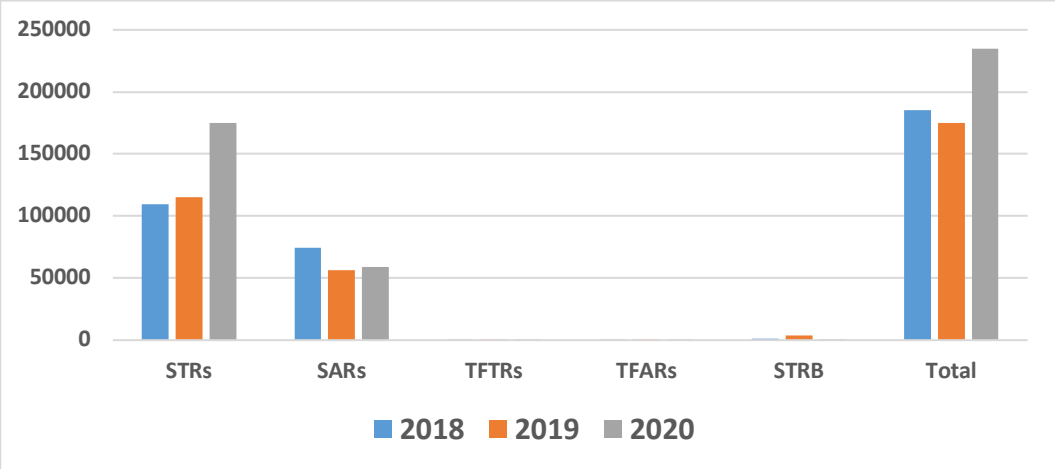
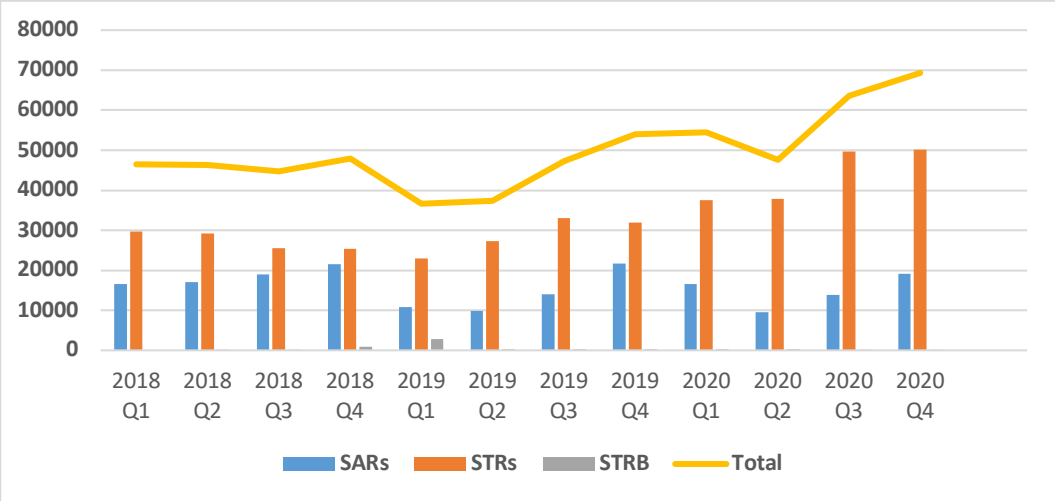


Figure 32: Number of section 29 reports processed by the FIC per quarter



Report indicators

The FIC uses report indicators to determine why the AIs and reporting institutions suspected some suspicious activity or transactions, and these are also used to determine predicate offences and for trend analysis. The table below depicts the top five risk indicators for SARs and STRs.

Table 51: Risk indicators in suspicious activity and transaction reports

Risk indicators: SARs	Risk indicators: STRs
1. SAR in terms of section 29 of the FIC Act	1. STR in terms of section 29 of the FIC Act
2. Activity does not match client profile or expected transacting patterns	2. Activity does not match client profile or expected transacting patterns
3. Fraud	3. Fraud
4. Large transfer of funds between accounts	4. Large electronic funds transfer
5. Reports filed because of a subpoena received in relation to a fraud investigation/case	5. Regular cash deposits

17.3.2 Types of suspected activities and predicate offences

The top three predicate offences that generated most of the laundered proceeds for 2018 to 2019 and 2019 to 2020 were:

- fraud;
- tax crimes and corruption; and
- bribery.

Other predicate offences highlighted by the FIC were:

- illegal gambling;
- robbery and theft; and
- terror financing.

17.3.3 FIC analysis of ML and TF typologies

From the analysis provided by the FIC, the following typologies were found to be linked to the section 29 reports submitted by the banking sector:

- When examining the preferred placement technique[43] from types of STRs, the FIC observed that drug traffickers were most likely to use smurfing and structuring techniques, fraudsters were most likely to use camouflage, and tax evaders favoured smurfing[44] and structuring.
- The use of shell or front companies is the preferred layering[45] technique employed by thieves, commodity traffickers, tax evaders and fraudsters. Tax evaders also preferred fake invoices as a layering technique.
- The integration phase technique is mostly used by money launderers to acquire the real estate . The establishment of an import/export business was equally preferred by tax evaders and drug traffickers.
- Thieves used the acquisition of luxury goods, purchase of cash incentive business, acquisition of real estate, as well as acquisition and smuggling of arms. On the other hand, human traffickers preferred to use only one method of integration, namely the purchase or use of cash-intensive businesses.

[43] The set of techniques used by money launderers to initially place illegal funds into financial system is referred as the placement techniques.
[44] Smurfing is a technique used by money launderers, for example by making bank deposits in a specific pattern calculated to avoid triggering financial institutions to file reports required by law.
[45] This method is often used by all types of money launderers using fake invoices and fictitious sales and purchases.

17.3.4 Red flags associated with the banking sector

The FIC provided the following list of red flags associated with the banking sector in South Africa:

- The client provides false, misleading or substantially incorrect information concerning the source of funds, or refuses to identify or fails to indicate a legitimate source of funds.
- The business involves foreign nationals, foreign bank accounts, government officials, or jurisdictions subject to the Office of Foreign Assets Control (OFAC) sanctions[46].
- The account sees an inflow of funds well beyond the known income or resources of the client.
- The client has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The client engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the R25 000 reporting threshold.
- For no apparent reason, the client has multiple accounts under a single name or multiple names, with many inter-account or third-party transfers.
- The client deposits funds and then immediately requests that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

18. Terrorist property reporting

18.1 Terrorist property reporting statistics

This section focuses on the assessment of quantitative data that was collected from the banking sector and the FIC in respect of terrorist property reports (TPRs). The

[46] Currently the Balkans, Burma, Ivory Coast, Cuba, Iran, Liberia, Libya, North Korea, Sudan, Syria and Zimbabwe.

banking sector reported five TPRs to the FIC for the period 1 October 2018 to 31 December 2020. Four of these were reported by locally controlled banks and one was reported by a large bank. The FIC received one alert for an individual listed on the UN Security Council targeted financial sanctions list.

Table 52: Terrorist property reporting by banks from 1 October 2018 to 31 December 2021

Categories of banks	TPRs reported	Total
Locally controlled banks	4	4
Large banks	1	1
Total	**5**	**5**

19. Observations from inspection outcomes

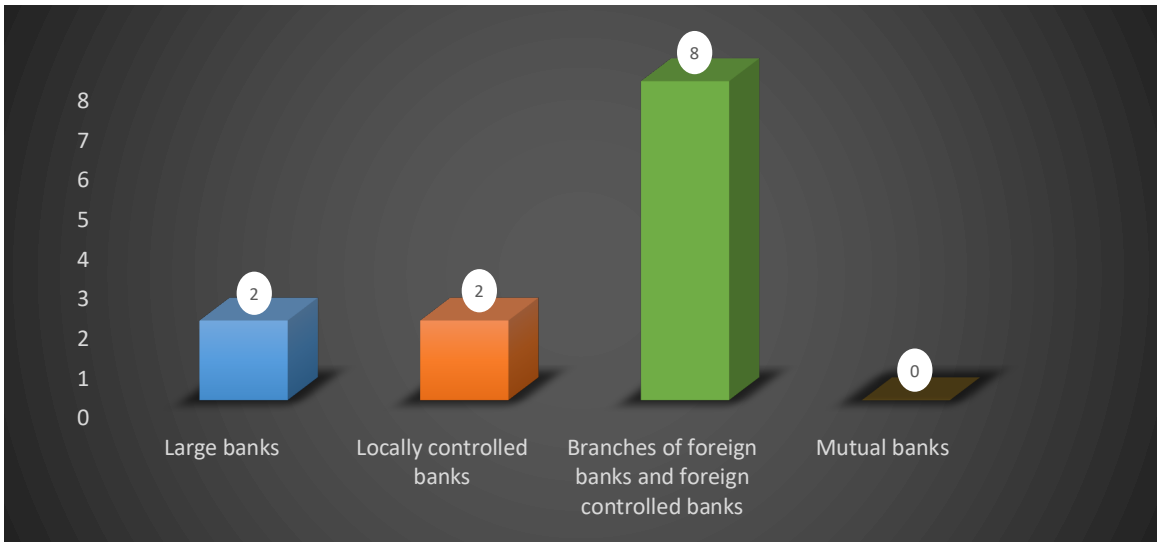
19.1 Introduction

The following section provides an overview of the risks identified from the AML/CFT inspections conducted at banks from October 2019 to September 2020. The overview will indicate the deficiencies identified, which denote ML/TF vulnerabilities.

19.2 Methodology

The PA conducted inspections in terms of the updated FIC Act from 2 April 2019. The PA commenced with the risk-based approach inspections in April 2019, following an 18-month grace period for AIs to fully implement the risk-based approach requirements of the FIC Act, effective on 2 October 2017. The analysis conducted are for the inspections conducted at banks from April 2019 to September 2020. The graph below provides further detail on the number of inspections.

Figure 33: Number of inspections conducted from April 2019 to September 2020

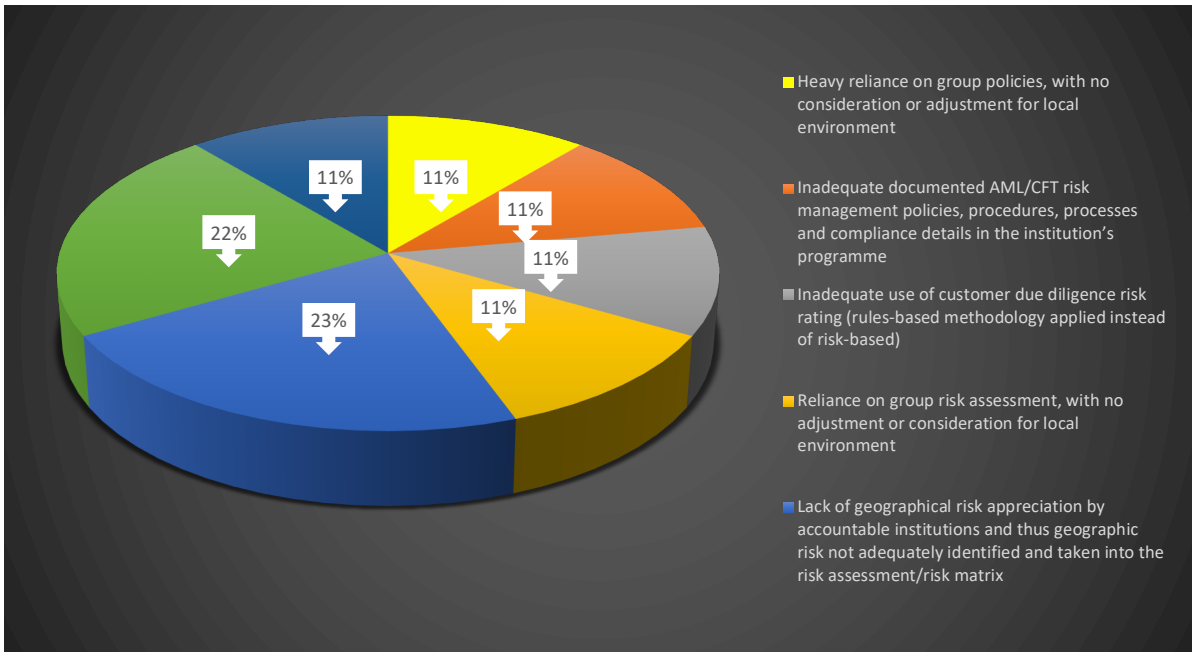


The purpose of the inspections was to assess the AI's level of compliance with the requirements of the FIC Act and any associated order, determination and/or directive. The detailed deficiencies found during inspections are outlined below.

19.2.1 Risk management and compliance programme

The objective was to establish whether the AIs had developed, documented, maintained and implemented a programme for AML and CFT risk management and compliance in terms of section 42. The deficiencies are outlined below.

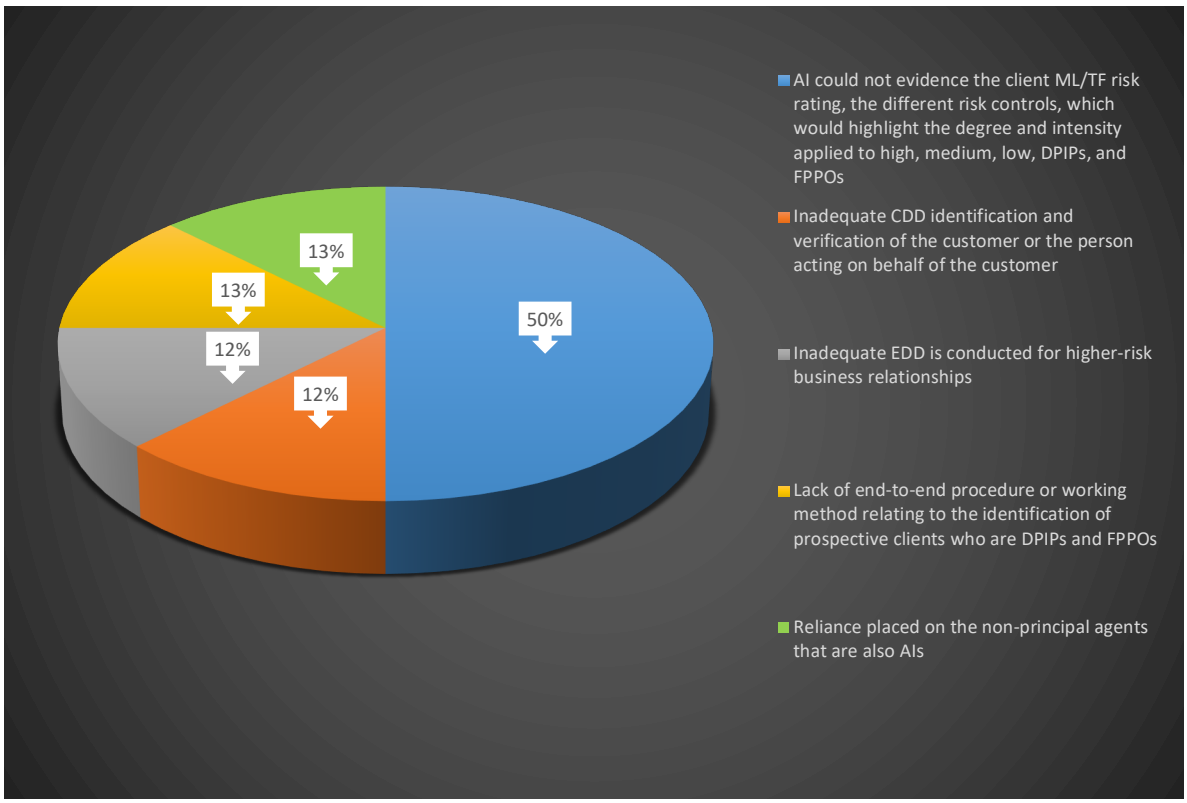
Figure 34: Deficiencies linked to risk management and compliance programme



19.2.2 Client due diligence and enhanced due diligence

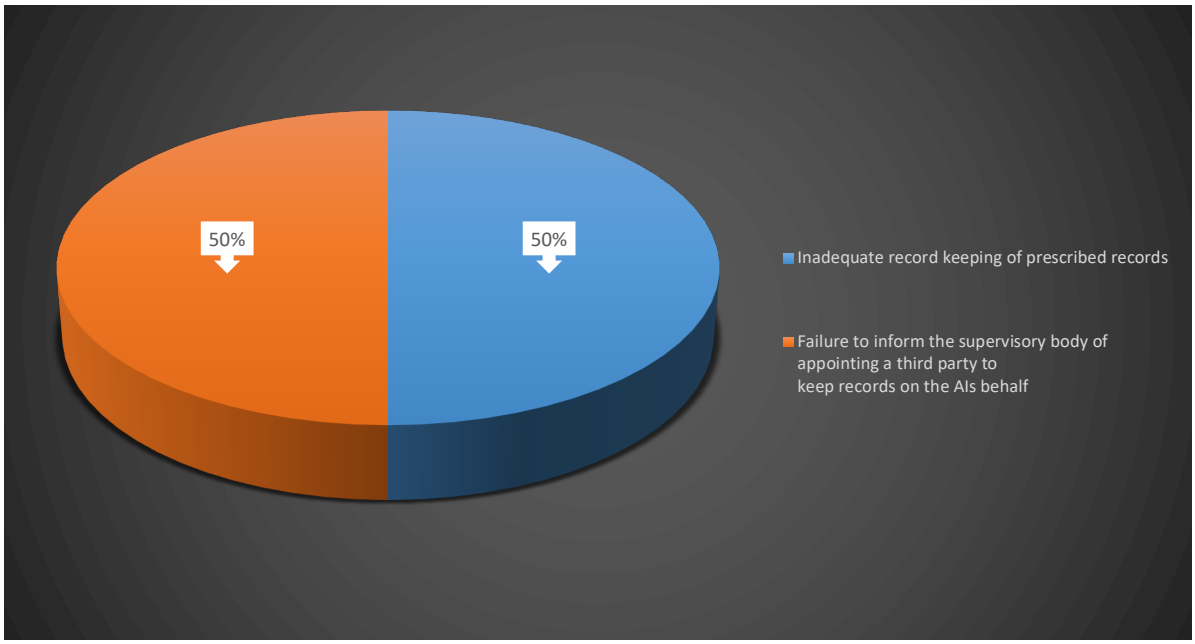
The objective was to establish whether the AIs complied with the requirements in terms of section 21 of the FIC Act. The deficiencies are highlighted in Figure 35.

Figure 35: Client due diligence and enhanced due diligence deficiencies



19.2.3 Record-keeping

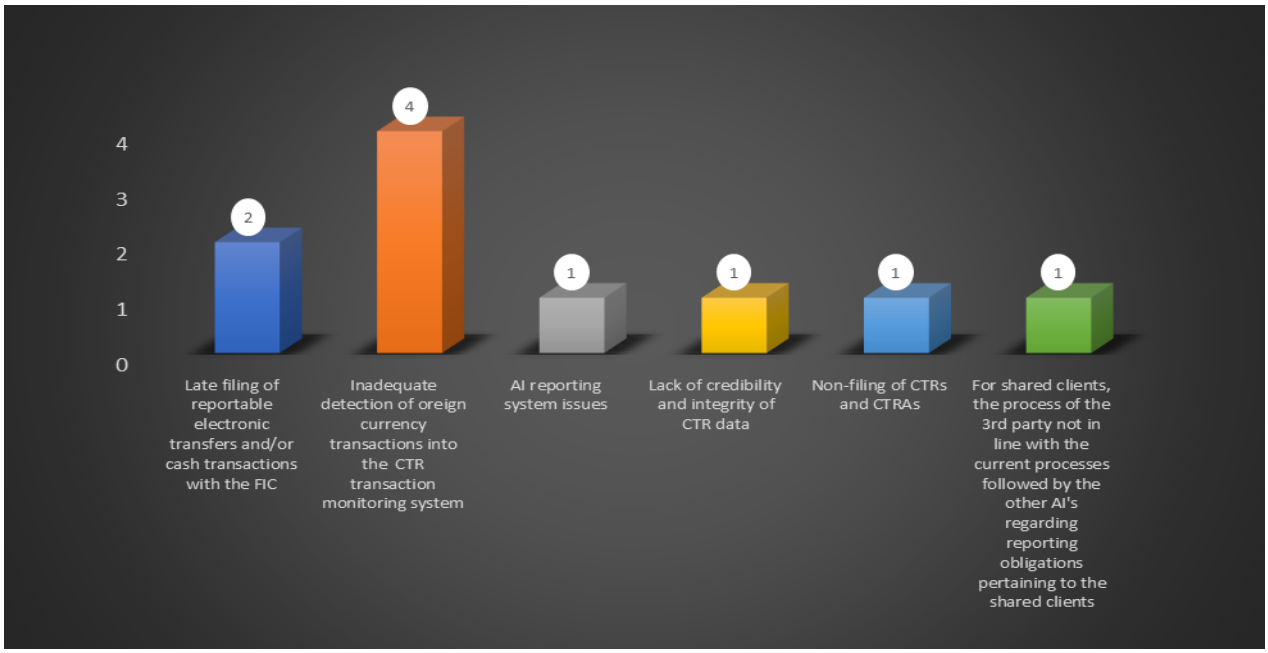
The objective was to establish whether the AIs had kept records of clients in accordance with the requirements outlined in the FIC Act and their risk management and compliance programmes. The deficiencies linked to record-keeping obligations are highlighted below.



19.2.4 Cash threshold reporting

The objective was to establish whether the AIs had complied with the provisions of sections 28 and 42 of the FIC Act. The deficiencies pertaining to cash-threshold reporting are highlighted below.

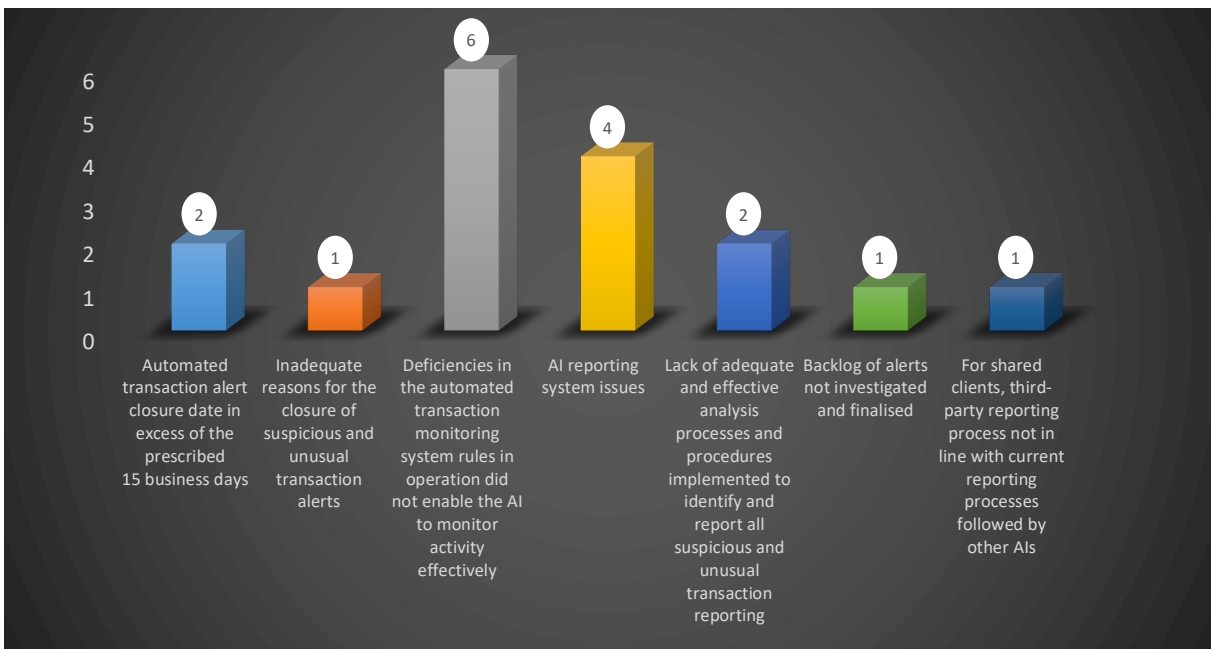
Figure 36: Cash threshold reporting deficiencies



19.2.5 Suspicious and unusual transactions

The objective was to establish whether the AIs had complied with the provisions of sections 29 and 42 of the FIC Act. The deficiencies linked to suspicious and unusual transaction reporting are highlighted below.

Figure 37: Deficiencies in reporting of suspicious and unusual transactions or activities



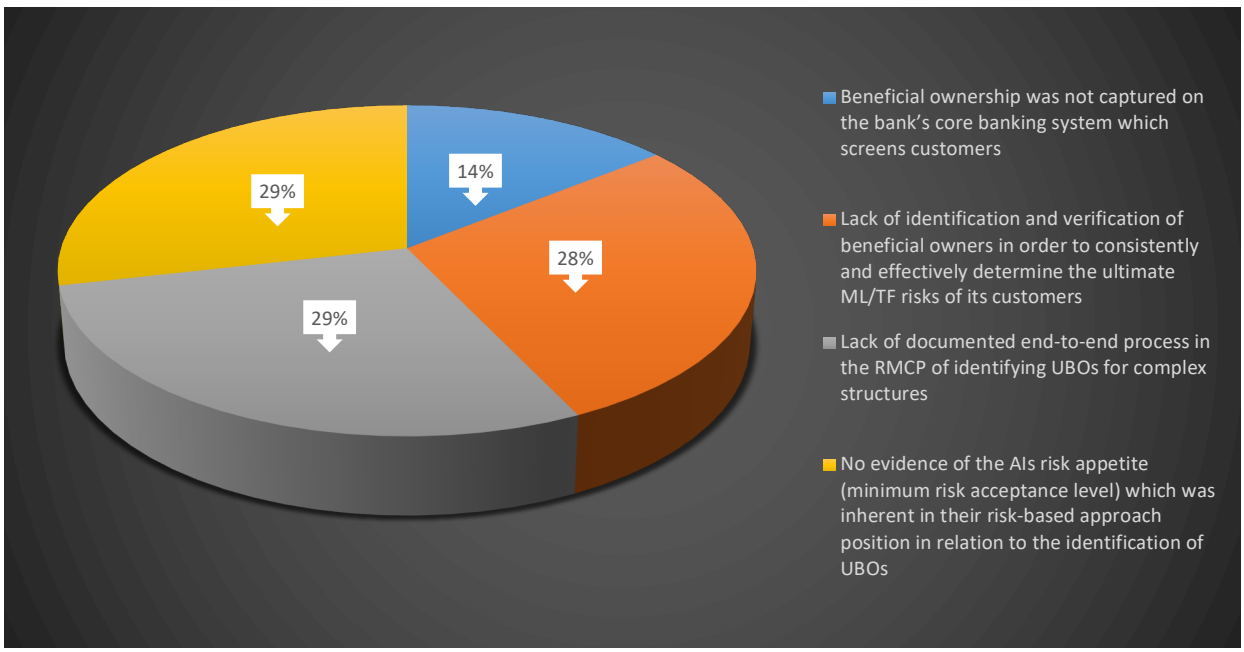
19.2.6 Ultimate beneficial ownership

The objective was to establish the level of compliance with section 21B(2), which requires AIs to establish the identity of the beneficial owner of the client. Transparency in respect of beneficial ownership reporting is a matter of concern as opaque and complicated ownership structures create the perfect setting to disguise the proceeds of unlawful activity, which can be used for illicit purposes and ML.

NPOs can be used to obtain funds (potentially through anonymous donors) for charitable organisations, and the flow of funds into and out of the NPO may be complex, making them susceptible to abuse by money launderers and terrorists.

AIs should gather additional information to help learn what type of activity to expect from the NPO regarding beneficial ownership, including general information about the donor base, funding sources and fundraising methods. It would be useful to have general information about beneficiaries and criteria for disbursement of funds, including the standards for qualifying beneficiaries and any intermediaries and their affiliation with other NPOs, governments or groups.

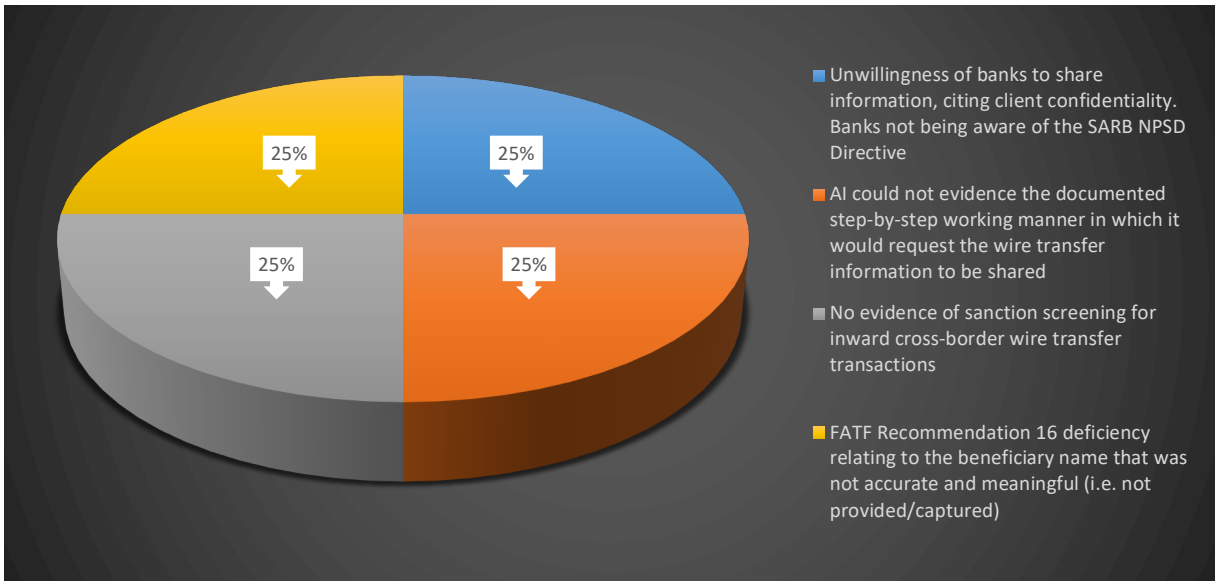
Figure 38: Ultimate beneficial ownership (UBO) deficiencies



19.2.7 Wire transfers

The objective was to establish whether the AIs implemented the SARB's National Payment System Department Directive 1 of 2015, read with the standard set out in FATF Recommendation 16, FIC guidance notes, and the risk management and compliance programme.

Figure 39: Wire transfer deficiencies



19.2.8 Other notable deficiencies identified include:

19.2.8.1 Governance and compliance function

The objective was to assess the level of compliance in terms of sections 42A(1) and (2). These sections require the Board of Directors (Board) of an AI – a legal person with a Board or the senior management of an AI without a Board – to ensure compliance by the institution and its employees with the provisions of the FIC Act and its risk management and compliance programme (RMCP).

Deficiency: inadequate oversight and monitoring relating to the FIC Act obligations.

19.2.8.2 Correspondent banking

The objective was to establish whether the AIs implemented the guidelines outlined in section 42 of the FIC Act, FATF Recommendations 1, 10 and 13, and the

Wolfsberg Group principles relating to EDD measures for high-risk relationships, such as correspondent banking.

Correspondent banking is inherently high risk due to the large amount of funds, the large volume of transactions, many ML fraud schemes, and the domestic bank's unfamiliarity with the foreign correspondent bank's clients, thus making it easy for criminals to conceal the source and use of ill-gotten funds.

- Client deficiency: CBRs did not comply with the EDD measures applicable to high-risk-rated CBRs in terms of the accountable institutions' RMCP.
- Risk: the CBR is prone to abuse as there is a lack of visibility into the governance of a respondent bank's clients for whom it does business.

19.2.8.3 AML/CFT training

The objective was to establish whether the AIs had complied with the obligation to provide ongoing training to their employees as required by section 43 of the FIC Act, FIC guidance note 7 and their RMCPs.

- Deficiency: the AIs could not show that the sampled employees have received refresher training.

  Risk: employees would be less likely to recognise red flags and suspicious activity, resulting in an environment more prone to ML/TF abuse.

20. Additional trends and typologies

20.1 Correspondent banking

Correspondent banking services are offered and utilised within South Africa. Many large South African banks have multiple relationships with foreign banks that clear transactions to enable payments in other currencies, for example, in US dollars and euros. Without established CBRs, it would be impossible for a bank in South Africa to effect payments on behalf of its clients abroad.

CBRs are quite critical. However, these relationships do present a risk to a bank providing the services. For South African banks holding nostro relationships with

foreign correspondent banks, confirmation from the foreign bank regarding the level of compliance by banks with FATF Recommendation 16 is often requested.

Figure 40: Number of correspondent banking relationships

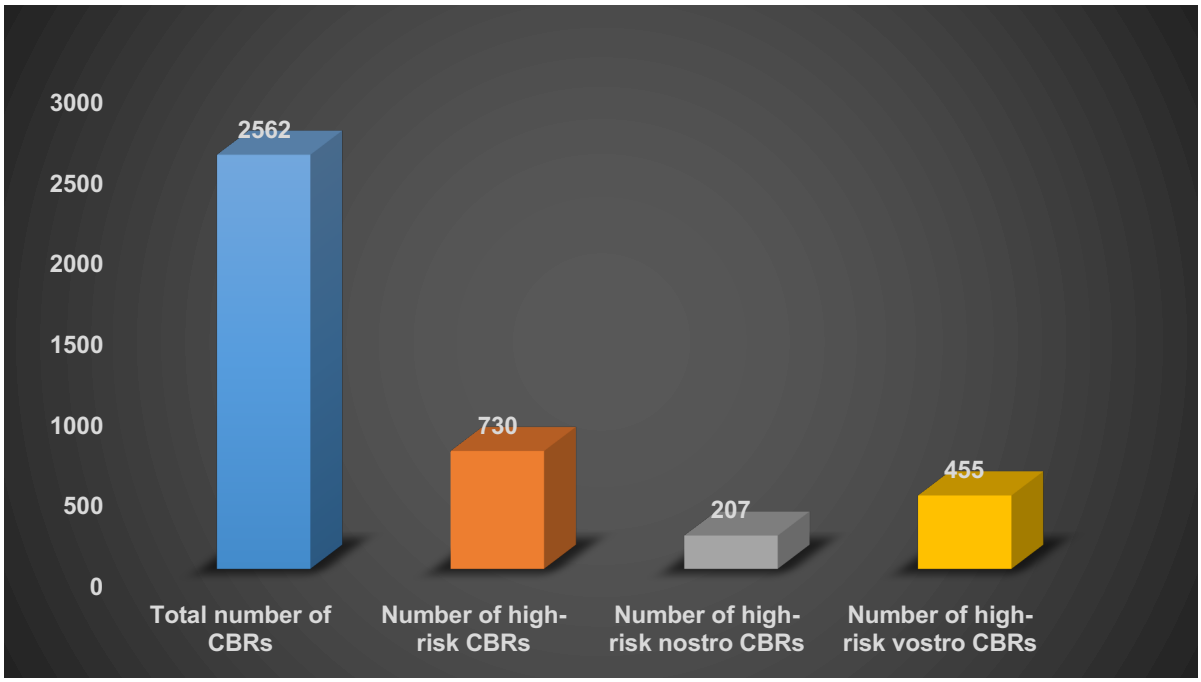


Figure 41: Number of high-risk CBRs

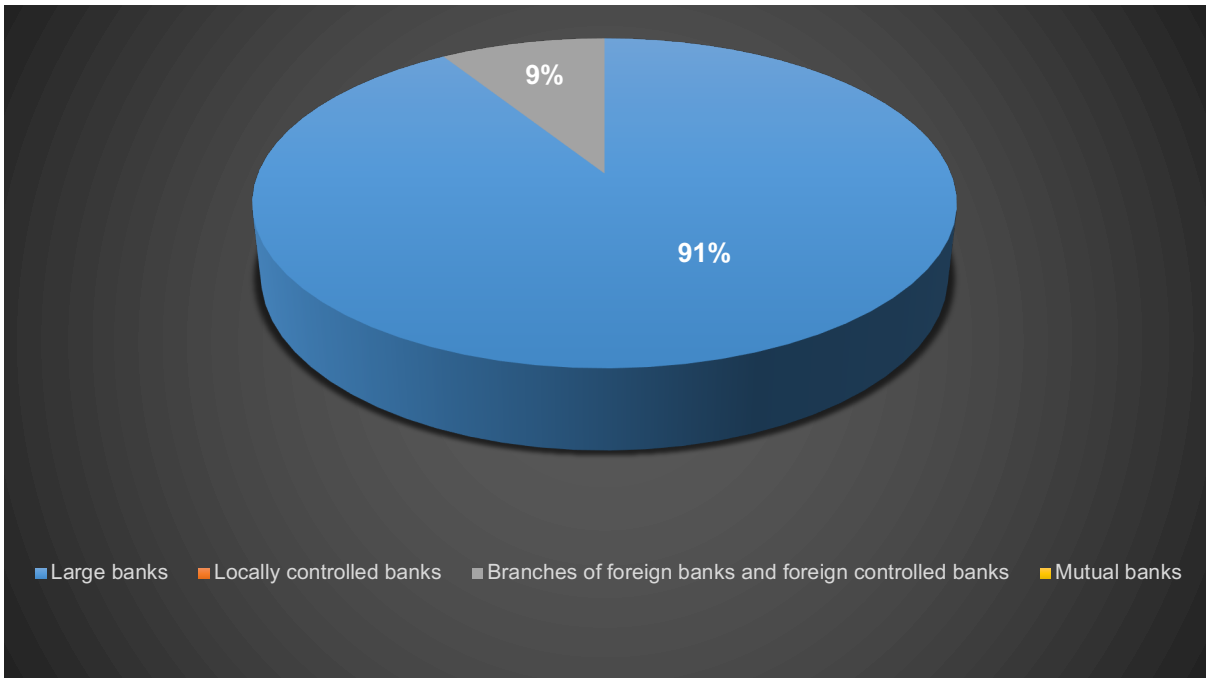


Figure 42: Number of high-risk nostro CBRs

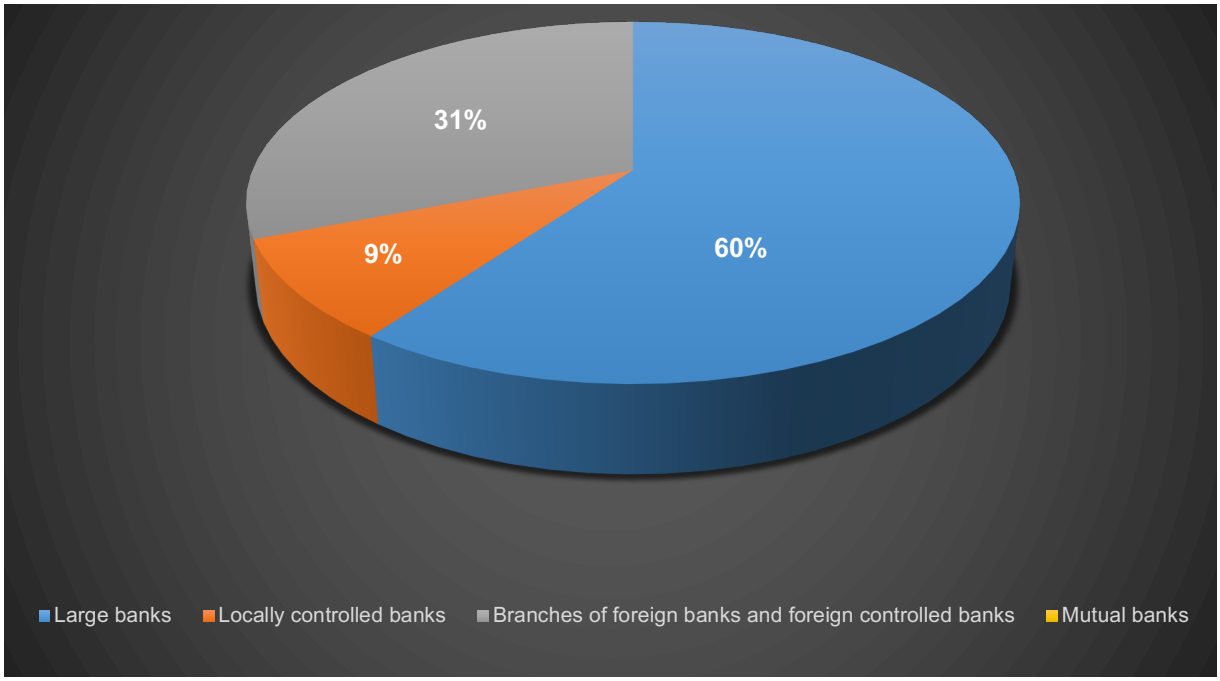
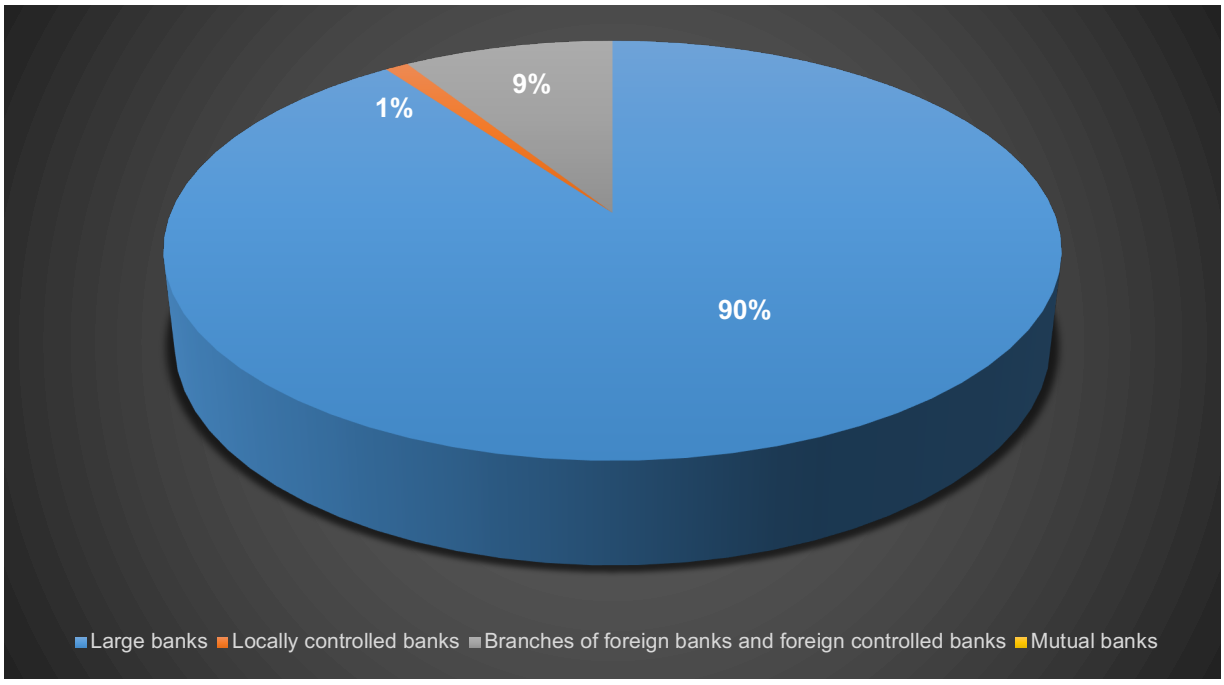


Figure 43: Number of high-risk vostro CBRs



Out of the 32 of the 34 registered banks that responded, 27 banks indicated that they prohibit financial institutions from maintaining relationships, including CBRs, with North Korean and Iranian financial institutions. Three branches of foreign

banks and foreign controlled banks indicated that they do prohibit this, whereas two recently registered locally controlled banks and the three mutual banks indicated that this was not applicable as they do not have CBRs.

20.2 Cross-border movement of funds

South Africa is a major player on the African continent as it has positioned itself as a regional financial hub. However, cross-border flows of funds have also been exploited by criminals through the placement, layering and integration of funds from illicit sources; and by terrorists from both legitimate and illegitimate sources to finance acts of terrorism.

Cross-border movements of funds can be seen as a form of global financial integration. It mainly involves flows of foreign direct investment, portfolio equity, trade finance and debt investment mostly aimed towards governments, multinational corporations, major financial institutions, and enterprises participating in international trade to and from South Africa. To a lesser extent, it also includes people investing offshore, purchasing foreign exchange for travel purposes, remitting money to family abroad and purchasing goods denominated in a foreign currency online. South Africa has over the years mostly had the same major trading partners, with a few newcomers as the global political and economic landscape evolves.

Following the 2019 FATF Mutual Evaluation, the FATF observed that:

- South Africa is a major financial hub, both in the region and on the continent, and a gateway for large financial flows between sub-Saharan countries and the rest of the world.
- The banking sector offers a diverse suite of products and services and provides access to the continent.
- The large banks have a broad regional network in sub-Saharan Africa as well as in global financial centres, including CBRs worldwide.
- South Africa is facing a relatively high volume and intensity of crime. The authorities have demonstrated an understanding of domestic ML threats, including those related to corruption, and associated vulnerabilities to some

extent, but their understanding of TF risks has been limited. Their lack of understanding of ML risks arising from foreign proceeds was a concern.

- Recent cases of 'state capture' highlighted the risks faced by South Africa with regard to proceeds of corruption and other financial crimes being laundered abroad.
- There were substantial cross-border financial and trade flows with Iran and North Korea.

20.2.1 Common risks: Cross-border movement of funds

The cross-border movement of funds by its nature poses ML/TF/PF risks, including threats and vulnerabilities. Banks which offered such services are responsible for monitoring the above-mentioned risks. Common risks within the sampled banks included:

- Clients were offered products with the ability to transfer funds across the border at a rapid rate and with high limits, for example transactional accounts.
- Banks were exposed to jurisdictions which presented higher ML/TF/PF risks as they were susceptible to predicate crimes such as corruption.
- Clients used complex and/or opaque structures, such as shell or front companies, or used fictitious documents and/or information.
- Complex transactions were used to disguise the nature and intended purpose of the funds. Furthermore, some transactions were structured to avoid reporting requirements and/or detection.

20.2.2 Common typologies, anomalies and trends

Various typologies, anomalies and trends were developed to monitor the flow of funds to and from South Africa, where known local and international syndicates were operating and using the country to launder ill-gotten gains. Banks provided the following examples:

- A personal account was used to receive inward cross-border SWIFT payments from one of the neighbouring countries. Upon detection and investigation, it was found the mode of operating was similar to a pyramid or Ponzi scheme. This suspicious behaviour was reported in terms of section 29 of the FIC Act.

- Trends indicated that African markets presented the highest risk when assessing clients transacting with entities in high-risk jurisdictions and whether any of the transactions were indicative of financial crime.
- Rapid movement of funds through a client's account was a red flag for possible ML activities, as criminals attempt to evade detection by creating complex processes to move illicit funds and layer them through multiple bank accounts. Clients with multinational footprints were found to have this transactional pattern and to be predominantly involved in or supporting the mineral resource industries.
- Major concerns and risk were identified pertaining to government consulting contracts (and by extension government business in general) won by professional services providers. These providers made payments to intermediaries located offshore, with little to no footprint, without logical commercial rationale before or shortly after fees were received. An example was a payment made from the funds received from the government by a client who won a tender for an undisclosed government institution. The client made a payment to a shell company in Mauritius and another to a local shell company. The Mauritius payment was returned to the client and paid to the local shell company. Another larger payment was made to the local shell company prior to receipt of another large government payment.
- Large deposits were made in a dormant account and then funds were transferred across the border.
- Inward transfers were received from foreign jurisdictions and vague information was provided about the relationship and purpose of the funds.
- Multiple cash deposits or EFTs in small amounts were made in an account, followed by a large wire transfer to another country.
- The account holder and/or the beneficiary were from countries known to support terrorist activities and organisations.
- Adverse publicity indicated that the account holder was linked to known terrorist organisations or was engaged in terrorist activities.
- A business was owned by people of the same nationality or by a business that involved people of the same country that are risk rated as high (such as

countries designated by national authorities and the FATF as non-cooperative countries and territories).

- Multiple personal, business, NPO or charity accounts received funds from various remitters and then funnelled funds to a small number of foreign beneficiaries.
- Foreign exchange transactions were made to locations having no apparent business connection with the client or to higher-risk countries.
- A client obtained a credit instrument or engaged in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appeared to be no logical business reasons for dealing with those locations.
- Wire transfers were made to areas of conflict.
- Financial activity identifiable with travel to sanctioned countries or countries regarded as high risk.

20.2.3 Cross-border movement of funds between South Africa and other jurisdictions

The following section outlines the top 15 jurisdictions with the highest total rand value in cross-border movement of funds with South Africa, including those that were regarded as financial secrecy havens between 2015 and 2018.

The Financial Secrecy Index,[47] launched on 18 February 2020, ranks jurisdictions according to their level of secrecy and the scale of their offshore financial activities. The index is a politically impartial ranking of jurisdictions, and a tool for understanding global financial secrecy, tax havens or secrecy jurisdictions, and illicit financial flows or capital flight.[48] It is regarded as the world's most

[47] Tax Justice Network. 2020. *Financial Secrecy Index*. Available at https://fsi.taxjustice.net/en/
[48] Ibid.

comprehensive review of the secrecy of global financial centres and the impact that this has on global financial flows.

The following table shows the 15 jurisdictions with the highest average outward flows from South Africa, including jurisdictions regarded as financial secrecy havens for 2015 and 2018.

Table 53: Average outward flows for 2015 to 2018

No.	Jurisdiction	Financial secrecy haven	Value in rand (R'000)
1	United Kingdom	No	R6 080 107 900
2	United States	Yes	R990 956 650
3	Belgium	No	R409 880 195
4	Germany	No	R192 761 504
5	Switzerland	Yes	R271 759 418
6	France	No	R157 286 203
7	Australia	No	R132 033 091
8	China	No	R109 598 537
9	Luxembourg	Yes	R87 679 764
10	Singapore	Yes	R78 152 381
11	Netherlands	Yes	R73 580 204
12	Hong Kong	Yes	R63 300 012
13	Mauritius	No	R60 014 768
14	Japan	Yes	R59 156 712
15	Austria	No	R55 242 727

The following table shows the 15 jurisdictions with the highest average inward flows to South Africa including jurisdictions regarded as financial secrecy havens for 2015 and 2018:

Table 54: Average inward flows for 2015 to 2018

No.	Jurisdiction	Financial secrecy haven	Value in rand (R'000)
1	United Kingdom	No	R6 265 737 150
2	United States	Yes	R1 358 493 125
3	Belgium	No	R265 575 604
4	Germany	No	R260 054 741
5	Switzerland	Yes	R226 643 126
6	France	No	R137 204 159
7	Australia	No	R127 913 709
8	Luxembourg	Yes	R78 283 536
9	Singapore	Yes	R74 541 031
10	Botswana	No	R52 635 565

11	Japan	Yes	R48 196 333
12	Mauritius	Yes	R46 820 400
13	Mozambique	No	R33 928 598
14	Netherlands	Yes	R36 146 842
15	United Arab Emirates	Yes	R44 335 118

20.2.4 Cross-border movement of funds with other financial secrecy havens

The following table shows the average inward and outward flows between South Africa and jurisdictions that are regarded as financial secrecy havens but did not form part of the top 15 jurisdictions.

Table 55: Average outward flows for 2015 to 2018

No.	Jurisdiction	Financial secrecy haven	Value in rand – outward (R'000)	Value in rand – inward (R'000)
1	Cayman Islands	Yes	R5 157 376	R4 371 909
2	British Virgin Islands	Yes	R495 470	R1 436 757

20.2.5 Cross-border movement of funds with FATF call-for-action jurisdictions

High-risk jurisdictions subject to a call for action have substantial strategic inadequacies in their regimes to counter ML/TF/PF.[49] Member countries are urged to apply enhanced due diligence and in certain instances apply countermeasures to protect the global financial system against the ongoing risk of ML/TF/PF from these jurisdictions. This list of high-risk jurisdictions is often referred to as the FATF 'blacklist'.[50]

[49] FATF. 2021. 'High-risk jurisdictions subject to a call for action – 21 February 2020'. Available at Documents - Financial Action Task Force (FATF) (fatf-gafi.org).
[50] Ibid.

20.2.5.1 Iran

- FATF strategic deficiencies: In October 2019, the FATF called on its members and urged all jurisdictions to require increased supervisory examination for branches and subsidiaries of financial institutions based in Iran; introduce enhanced relevant reporting mechanisms or systematic reporting of financial transactions; and require increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in Iran.[51]
- UN and TF conventions: Upon Iran's failure to enact the UN Convention against Transnational Organized Crime (or Palermo Convention)[52] and TF Convention[53] in line with the FATF Standards, the FATF called on its members and urged all jurisdictions to apply effective countermeasures, in line with Recommendation 19.[54] The purpose of the Palermo Convention is to promote cooperation to prevent and combat transnational organised crime more effectively.[55]
- Sanctions: Iran is sanctioned by the UN, European Union and the US.[56] On 10 January 2020, the US fully reinstated its nuclear-related sanctions waived under that agreement[57], including banning foreign subsidiaries of US companies from dealing with Iran and imposing secondary sanctions on foreign companies that engage in certain Iran-related transactions. The UN Security Council unilaterally declared the reimposition of all UN sanctions[58] against

[51] FATF. 2019. 'FATF Public Statement – October 2019'. Available at Documents - Financial Action Task Force (FATF) (fatf-gafi.org).
[52] Refers to the UN Convention adopted by the General Assembly. 'Convention against Transnational Organized Crime and the Protocols thereto. Available at: United Nations Convention against Transnational Organized Crime and the Protocols thereto (unodc.org).
[53] Refers to the UN Convention adopted by the General Assembly. 'International Convention for the Suppression of the Financing of Terrorism adopted on 9 December 1999'. Available at International Convention for the Suppression of the Financing of Terrorism (un.org).
[54] KnowYourCountry, Iran, FATF Statement – 21 October 2021. Available at: Iran, Islamic Republic of – KnowYourCountry.
[55] See note 49 above.
[56] See note 49 above.
[57] Refers to the Joint Comprehensive Plan of Action adopted on 14 July 2015. Available at: Joint Comprehensive Plan of Action (state.gov).
[58] The UN Security Council has adopted seven resolutions as part of international efforts to address Iran's nuclear programme.

Iran.[59] In addition to a conventional arms embargo, then US Secretary of State Mike Pompeo said UN member states must comply with restrictions such as the ban on Iran engaging in nuclear enrichment and reprocessing-related activities; the prohibition on ballistic missile testing and development; and sanctions on the transfer of nuclear and missile-related technologies.[60]

20.2.5.2 North Korea

- FATF strategic deficiencies: The FATF had serious concerns about the threat posed by North Korea's illicit activities related to the proliferation of weapons of mass destruction and its financing.[61] The FATF further called on its members and urged all jurisdictions to apply effective countermeasures, and targeted financial sanctions in accordance with applicable UN Security Council resolutions, to protect their financial sectors from risks of ML, financing of terrorism and financing of weapons of mass destruction proliferation from North Korea. Jurisdictions should have taken necessary measures to close existing branches, subsidiaries and representative offices of North Korean banks within their territories and terminated correspondent relationships with North Korean banks, where required by relevant UN Security Council resolutions.[62]
- Sanctions: North Korea is sanctioned by the UN, European Union and the US.[63] Sanctions primarily target the direct or indirect supply of conventional weapons and certain weapons of mass destruction, sensitive goods and technology, and technical assistance. The US Treasury Department is authorised to sanction foreign banks that engage in significant transactions with North Korea and to block specific bank accounts linked to North Korea.[64] North Korea continued to

[59] M Motamedi. 2020. 'US claims UN sanctions on Iran reinstated', Al Jazeera article, 20 Sep 2020. Available at: US claims UN sanctions on Iran reinstated. The world disagrees | United Nations News | Al Jazeera.
[60] Ibid.
[61] See note 56 above.
[62] See note 56 above.
[63] FATF. 2021. 'KnowYourCountry, North Korea, FATF Statement – 21 October 2021'. Available at North Korea – KnowYourCountry.
[64] Ibid.

expand its nuclear and ballistic missile programmes and has tapped into illicit maritime networks, such as those near China and Taiwan, that allow North Korea to import refined fuel products and crude oil and to export revenue-generating coal.[65]

The following table depicts the average outward and inward flows between South Africa and FATF high-risk jurisdictions between 2015 and 2018.

Table 56: Average outward flows for 2015 to 2018

No.	Jurisdiction	FATF high-risk country	Value in rand – outward (R'000)	Value in rand – inward (R'000)
1	Iran	Yes	R134 846	R2 328 778
2	North Korea	Yes	R5 730 202	R2 456 789

20.2.6 Cross-border movement of funds with jurisdictions with a higher risk of terrorism

The following table outlines the value of inward and outward flows between South Africa and the top 10 jurisdictions with the highest score for the impact of terrorism for the year 2020. The score for terrorism is based on the Global Terrorism Index, a comprehensive review that analyses the impact of terrorism across 163 jurisdictions covering 99.7% of the world's population.[66] The index considers longer-term trends, how terrorism changes over time, the geopolitical drivers associated with terrorism, the ideological aims of terrorist groups, and the types of strategies deployed by terrorists, their tactical targets and how these have evolved over time. It defines terrorism as "the threatened or actual use of illegal force and violence by a non-

[65] S-M Kim. 2021. 'North Korea keeps evading UN sanctions'. *Arms Control Association* May 2021. Available at North Korea Keeps Evading UN Sanctions | Arms Control Association accessed on 31 October 2021.

[66] Institute for Economics & Peace. 'Global Terrorism Index 2020: Measuring the impact of terrorism', Sydney, November 2020. Available at https//visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf accessed on 2021-10-28.

state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation".[67]

Table 57: Cross-border movement of funds between South Africa and high-risk TF jurisdictions – outward

No.	Jurisdiction	FATF: Jurisdictions under increased monitoring	Value in rand – outward (R'000)
1	India	No	R41 070 955
2	Nigeria	No	R26 204 484
3	Democratic Republic of Congo	No	R7 054 336
4	Pakistan	Yes	R3 424 691
5	Mozambique	No	R804 100
6	Afghanistan	No	R283 894
7	Somalia	No	R23 116
8	Iraq	No	R19 910
9	Syria	Yes	R7 331
10	Yemen	Yes	R5 027

Table 58: Cross-border movement of funds between South Africa and high-risk TF jurisdictions – inward

No.	Jurisdiction	FATF: Jurisdictions under increased monitoring	Value in rand – inward (R'000)
1	Nigeria	No	R26 833 229
2	India	No	R17 494 159
3	Democratic Republic of Congo	No	R5 685 961
4	Mozambique	No	R962 959
5	Pakistan	Yes	R298 506
6	Iraq	No	R180 210
7	Afghanistan	No	R139 859
8	Somalia	No	R122 766
9	Syria	Yes	R20 642
10	Yemen	Yes	R15 155

[67] Ibid, p. 6.

20.2.7 Methods and practices

20.2.7.1 Nature of persons or entities involved

Mostly newly registered local entities were used, without a record of previous cross-border transactions. Large values of funds were transferred abroad immediately after an entity was registered. In certain instances, dormant and shelf entities were also used.

20.2.7.2 Beneficial ownership

Entities with different bank accounts were mostly owned, controlled or managed by the same individuals to avoid detection by scattering outward payments. In certain instances, registered owners or managers had no role in an entity's banking activities. Registered owners of entities may have been used to disguise the identity of the real owners.

20.2.7.3 Financial transactions

Rand-denominated bank accounts were funded immediately before foreign exchange transactions were settled. Small amounts were kept in these accounts between foreign exchange transactions. These rand-denominated bank accounts were exclusively used for foreign exchange business and were funded mostly by cash deposits at different locations across the country. Electronic transfers were also used in certain instances where other local entities – which had no relationship with the entity in question – would transfer funds electronically. Cash was also deposited and then immediately transferred electronically. In some instances, the same owners or managers were not present across different accounts, but the same individuals were authorised signatories. Funds were transferred between multiple bank accounts before the foreign exchange settlement occurred. New entities were created in response to accounts being blocked.

20.2.7.4 Documentation and types of transactions

In most instances, supporting documents were fraudulent. In terms of trade transactions, the value of the actual imported goods did not correspond to the actual outward payment. Import and freight payments were used to disguise the actual purpose of foreign exchange transactions as no goods were ever cleared for importation. Payments to non-resident suppliers of goods in respect of merchant transactions were declared; however, no payment had been received from buyers. The use of foreign exchange intermediaries or treasury outsourcers also proved to be popular.

Payments were made to third parties, not the actual importer, on the instruction of local importers. In certain instances, third parties were individuals who were allegedly directors of foreign supplier companies. Payments were mostly made to bank accounts in Hong Kong where the supplier was in China.

Cardholders of locally issued credit and debit cards provided their cards to third parties – South African residents or foreign nationals, who used these cards abroad to withdraw cash. These card accounts were funded locally through cash deposits and/or electronic transfers. In most instances, multiple cards were issued under a single account number.

20.2.8 Law enforcement investigations

Law enforcement agencies focused mostly on high-profile cases where high-value outward movement of funds had been identified. These agencies, aimed to improve cooperation among themselves, focus on emerging illicit financial flow trends, make recommendations on threat assessment and increase the number of cases under investigation linked to professional ML, corruption and illicit trade.

At the time of the PA's analysis, law enforcement agencies had identified the following predicate offences related to illicit financial flows which were under enhanced scrutiny:

- Ponzi schemes;
- exchange control contraventions;

- illegal wildlife trade;
- hawaladar;
- cash seizures at ports of entry;
- corruption; and
- offences committed by international organised crime syndicates.

20.2.9 Transaction categories

The table below outlines transaction categories that were more susceptible to illicit financial flows, with estimated values for the period 2017 to 2020.

Table 59: Transaction categories more susceptible to illicit financial flows

Transaction categories	Estimated values
Advance payment for imports	R7 000 million
Import payments	R1 500 million
Merchant transactions	R3 000 million
Freight payments	R250 million
Third-party cash withdrawals using credit/debit cards	R2 700 million
Crypto assets	R5 000 million
Payment for services	R500 million

20.2.10 Examples of ML

The table below outlines examples of ML in relation to illicit financial flows with estimated values for the period 2017 to 2020.

Table 60: Examples of ML in relation to illicit financial flows

Examples	Estimated values
Alleged ML scheme involving smuggling precious metals	R1 600 million
Virtual asset service providers' accounts possibly abused for money mule purposes	R1 000 million
A syndicate abused the advance payment dispensation by establishing numerous companies that transferred vast amounts of foreign currency from South Africa	R150 million
Abuse of specialist payment solutions to facilitate payments for travel-related services	R1 700 million

20.3 State-owned entities[68]

Corruption is contrary to good governance and is a direct threat to government initiatives and the public interest. In terms of ML/TF/PF risks linked to the state-owned entities banked by accountable institutions, the following were observed:

- supply chain irregularities;
- tender irregularities, flouting of procurement processes and conflicts of interest;
- internal fraud or theft;
- kickbacks, self-enrichment by staff or bribery;
- corruption or mismanagement of funds;
- non-compliance with internal procedures and policies;
- maladministration;
- potential gross manipulation of contractual agreements between contractors, state-owned entity employees and third parties unduly benefiting from contracts;
- potential tax fraud charges relating to state-owned entity executives and employees; and
- potential ML, and the offer and receipt of unauthorised gratifications in connection with corruption and fraud cases.

20.4 Corruption[69] and state capture[70]

The concept of state capture was defined in a 2003 World Bank report on corruption in eastern Europe and central Asia.[71] Accountable institutions deal with

---

[68] A state-owned enterprise is a legal entity created by a government to partake in commercial activities on the government's behalf.

[69] Corruption, as it is defined by the World Bank, is a form of dishonesty or a criminal offence which is undertaken by a person or an organisation entrusted with a position of authority to acquire illicit benefits or abuse power for private gain.

[70] State capture describes a form of corruption in which businesses and politicians conspire to influence a government's decision-making process to advance their own interests.
State capture: Zuma, the Guptas, and the sale of South Africa – available at https://www.bbc.com/news/world-africa-48980964

client relationships implicated in corruption and state capture through the following measures:

- Corruption and state capture continue to be discovered through various commissions of enquiries. Accountable institutions consider and respond to the outcome of enquiries by investigating allegations against their banking relationships.
- The accountable institutions monitor the news on an ongoing basis to identify clients who might be linked to allegations of fraud or corruption.
- If subjects of interest are identified, further analysis and monitoring is conducted on the relevant accounts.
- Details relating to personal protective equipment corruption have also been shared with the Fusion Centre as part of the South African Anti-Money Laundering Integrated Task Force (SAMLIT) Tactical Operating Group focusing on allegations of fraud and corruption around the awarding of tenders during the coronavirus pandemic.
- Accountable institutions have implemented additional monitoring mechanisms, such as developing an exception report highlighting possible transactions of concern during the lockdown period, reviewing various lists published by National Treasury and government departments, and reviewing transactional flows from municipality accounts.
- Accountable institutions ensured that the relevant regulatory reports – on suspicious transactions and activity – were filed with the FIC. This may also cause the clients' AML/CFT risk ratings to be manually upgraded to high risk, coupled with an enhanced due diligence review of the business relationship, which could result in the clients being referred to a high-level committee for consideration. The change to a high-risk rating would also entail closer monitoring of the clients' accounts.

20.5 Financial technology and virtual asset service providers

20.5.1 Financial technology

Financial technology (fintech) is an emerging industry where technology and innovation aim to compete with traditional financial methods in the delivery

of financial services that uses technology to improve activities in finance. Fintech services may originate from various independent service providers, including at least one licensed bank or insurer. The interconnection is enabled through open application programming interfaces and open banking.

20.5.2 Virtual asset service providers

A virtual asset service provider conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets;
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Virtual assets enable non-face-to-face business relationships. They are used to move funds around the world quickly and to facilitate a range of financial activities: from money or value transfer services to securities, commodities or derivatives-related activity. The absence of face-to-face contact in virtual asset financial activities or operations may indicate higher ML/TF/PF risks. Similarly, virtual asset products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher ML/TF/PF risks, particularly if they inhibit a virtual asset service provider's ability to identify the beneficiary. The latter is especially concerning in the context of virtual assets, which are cross-border in nature. If user identification and verification measures do not adequately address the risks associated with non-face-to-face or opaque transactions, the ML/TF/PF risks increase, as does the difficulty in tracing the associated funds and identifying transaction counterparties.

A virtual asset permits greater secrecy than traditional non-cash payment methods as it is characterised by non-face-to-face business relationships with potentially anonymous funding, transfers and transactions. These assets operate on a

decentralised system with no user identification information. Clients can freely trade, transfer and transact with virtual assets without ever being identified and verified. This is not the case with conventional online payment and trading platforms.

There is presently no AML transaction monitoring system that can monitor all virtual asset transactional behaviour and patterns and determine if it is suspicious in nature. Each transaction is added on an encrypted chain of transactions. The transactional history is recorded on distributed ledgers, which are maintained in a decentralised format (no central database administrator) across different users and jurisdictions. It is difficult for law enforcement agencies to identify, investigate, prosecute and convict people that use virtual assets for unlawful activities as there is no central authority, intermediary or administrator to approach. Nonetheless, law enforcement agencies usually approach specific virtual asset service providers that do collect client information to enable them to fulfil their functions.

Virtual assets are transacted over the internet across international borders, which heightens ML/TF/PF risk. The virtual asset system reaches many people, entities and jurisdictions that use it for investment, trade and transactions. Transactional and client data may also be held by different entities in different jurisdictions. Regulation, supervision and enforcement is difficult due to the complexity and technical nature of such transactions.

The inherent risks of virtual asset service providers have not been assessed nor are they regulated or supervised in South Africa. The majority of banks view virtual asset service providers as high-risk clients and prefer not to conduct business with them. The perception is that virtual assets are primarily used for unlawful activities. Only the large banks understood the ML/TF and PF threats and vulnerabilities associated with these service providers. Most banks choose not to onboard virtual asset service providers since they do not understand the ML/TF/PF risks linked to them.

Of the five large banks, one bank monitors crypto purchases and sales as well as cross-border crypto transactions, while another has developed a crypto model that is being refined to detect suspicious and unusual crypto-related transactions.

20.6 Cybercrime

Cybercrime may harm someone's security and financial health. Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion and theft of classified information. These types of crime often result in the loss of private information or monetary information. The following trends were identified in the South African Banking Risk Information Centre (SABRIC) annual report for 2020.[72] Cybercrime is on the rise in South Africa, with ransomware payments being demanded by cybercriminals[73]. A study by Surfshark using FBI data to develop an index, revealed South Africa to be seventh in terms of the number of cybercrime victims.[74]

2.6.1 COVID-19 scams

These scams included spoof emails from seemingly reputable companies, manipulating people into clicking on links. They offered products such as masks or fake offerings of vaccines that directed unsuspecting victims to phishing websites. These websites asked users to provide personal information that ended up in the hands of cybercriminals.

20.6.2 Compromised business emails

Criminals used information from company websites and/or other digital platforms to identify details relating to key senior individuals in the company. They would then

[72] SABRIC Crime Statistics 2020 – https://www.sabric.co.za/media/20oouwbg/sabric-annual-crime-stats-2020.pdf
[73] https://mybroadband.co.za/news/security/443728-south-african-companies-getting-nailed-by-ransomware-and-they-are-paying-up.html
[74] https://mybroadband.co.za/news/security/443090-cybercriminals-love-south-africa-study.html

impersonate these individuals, sending electronic requests via email or text message to junior staff in the accounting or finance function instructing for an urgent payment to be made to a specific beneficiary.

20.6.3 Phishing, vishing and smishing

Phishing (email), vishing (phone) and smishing (text) are all social engineering tactics used by criminals designed to manipulate victims into disclosing their confidential information such as their personal identification numbers and passwords to access their bank account. SABRIC reported that digital banking fraud increased by 33% in 2020. As clients turned to online shopping and settling payments on digital platforms, criminals also enhanced their efforts to steal personal data to defraud people on online platforms.

20.6.4 Debit order fraud

In terms of the SABRIC report, debit order fraud pertains to unauthorised debit orders of smaller amounts that usually go on undetected, and these are usually targeted at unemployed people, the elderly and people that receive grants. However, banks and the Payment Association of South Africa (PASA) have taken control measures to protect clients, such as introducing DebiCheck, a system that authenticates collections and requires the client to directly approve the processing of a debit order on his or her account.

20.6.5 Changes in card usage

SABRIC reported that credit card fraud decreased by 27% from 2019 to 2020, while debit card fraud increased by 22% for the same period. This was prompted by the uncertain economic conditions in South Africa, where clients used their debit cards with the funds in their account, rather than spending on their credit cards which they would have to pay back later.

The banking sector has been assessed as follows from an inherent risk perspective.

Table 61: Inherent risk assessment on additional trends and typologies

	Large banks	Locally controlled banks	Branches of foreign banks or foreign controlled banks	Mutual banks
Correspondent banking	High	Medium	High	Low
Illicit flow of funds	High	High	High	Low
State-owned entities	High	Medium	Medium	Low
Corruption and state capture	High	High	High	Medium
Fintech or virtual asset service provider	High	Medium	Low	Low
Cybercrime	High	High	High	High

Overall risk: High

21. Engagements with other stakeholders

21.1 National Prosecution Authority

The prosecuting authority is governed by the National Prosecuting Authority Act 32 of 1998. The Constitution, read with this act, empowers the prosecuting authority to institute criminal proceedings on behalf of the state and to carry out any functions necessary to institute criminal proceedings.

Table 62: Statistics linked to ML cases

Year	Standalone convicted cases	Standalone acquitted cases	Third-party laundering acquitted cases	Third-party laundering convicted cases	Self-laundering convicted cases	Self-laundering acquitted cases
2018/2019	87	0	0	0	0	0
2019/2020	72	1	0	0	0	0
2020/2021	22	2	0	16	24	2
Total	**181**	**3**	**0**	**16**	**24**	**2**

21.2 South African Revenue Service

The South African Revenue Service (SARS) is the nation's tax collecting authority. Established in terms of the South African Revenue Service Act 34 of 1997 as an autonomous agency, the service is responsible for administering the South African tax system and customs service. It provided the following statistics relating to tax fraud and tax evasion.

Table 63: Tax fraud and tax evasion statistics from SARS

Tax year	New cases received	Reactivated cold cases	Abandoned cases	Cases where action short of prosecution was taken	Cases referred for prosecution	Cases where prosecution was commenced	Number of convictions	Number of acquittals
2017	472	730	130	47	332	447	165	9
2018	569	539	59	16	411	397	84	4
2019	563	505	0	28	459	396	151	2
2020	528	756	4	16	500	559	130	2
2021	914	515	80	30	377	376	52	2

22. Risk assessment results (overall risk rating)

Table 64: Overall risk rating

Category of banks	Asset size	Client risk	Products risk	Delivery channel	Geographical risk	TF risk	PF risk	Other risk factors
Overall risk category	High	High	High	High	High	High	High	High

Overall risk: High

Abbreviations	
AI	accountable institution
AML	anti-money laundering
ATM	automated teller machine
CBR	correspondent banking relationship
CDD	client due diligence
CFT	counter-financing of terrorism
CPF	counter-proliferation financing
CTR	cash threshold report
CTRA	cash threshold report aggregation
DPIP	domestic prominent influential person
EDD	enhanced due diligence
EFT	electronic funds transfer
FATF	Financial Action Task Force
Fintech	financial technology
FPPO	foreign prominent public official
GN	Guidance Note
ML	money laundering
NPO	non-profit organisation
PA	Prudential Authority
PEP	politically exposed person
PF	proliferation financing
POS	point of sale
SARB	South African Reserve Bank
SARS	South African Revenue Service
TF	terror financing

Glossary

BANKS
Large banks
• Absa Bank Limited
• FirstRand Bank Limited
• Investec Bank Limited
• Nedbank Limited
• Standard Bank South Africa Limited
Medium to small locally controlled banks
• African Bank Limited
• Bidvest Bank Limited
• Capitec Bank Limited
• Discovery Bank Limited
• Grindrod Bank Limited
• Ithala SOC Limited
• Sasfin Bank Limited
• TymeBank Limited
• Ubank Limited
Branches of foreign banks and foreign controlled banks
• Access Bank South Africa Limited
• Al Baraka Bank Ltd
• Bank of China Limited – JHB branch
• Bank of Communications Co. Ltd – JHB branch
• Bank of Taiwan – South Africa branch
• BNP Paribas – South Africa branch
• China Construction Bank Corporation – JHB branch
• Citibank NA
• Deutsche Bank AG
• Goldman Sachs International Bank – JHB branch
• Habib Overseas Bank Ltd
• HBZ Bank Limited
• HSBC Bank Plc – JHB branch
• ICICI Bank Limited
• JPMorgan Chase Bank – JHB branch
• Standard Chartered Bank
• State Bank of India

Mutual banks
• Bank Zero Mutual Bank
• Finbond Mutual Bank
• GBS Mutual Bank

Terminology[75]

Consequence: refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML or TF may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector.

Predicate offence: for the purpose of this risk assessment, a predicate offence is any crime/unlawful activity.

Threat: A threat is a person or group of people, object or activity which has the potential to cause harm to, for example, the state, society, the economy and so forth. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities. Threat is described above as one of the factors related to risk, and typically it serves as an essential starting point in developing an understanding of ML/TF risk. For this reason, understanding the environment in which predicate offences are committed and the proceeds of crime are generated, to identify their nature (and if possible, the size or volume) is important in order to carry out an ML/TF risk assessment. In some instances, certain types of threat assessments might serve as a precursor for a ML/TF risk assessment.

Vulnerabilities: The concept of vulnerabilities as used in a risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities as distinct from a threat means focusing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes.

Applicable legislation

- Banks Act 94 of 1990
- Financial Sector Regulation Act 9 of 2017
- Mutual Banks Act 124 of 1993
- Companies Act 71 of 2008

[75] FATF: https://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

• the National Payment System Act 78 of 1998
• Financial Intelligence Centre Act 38 of 2001
• Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004