



Financial
Intelligence Centre

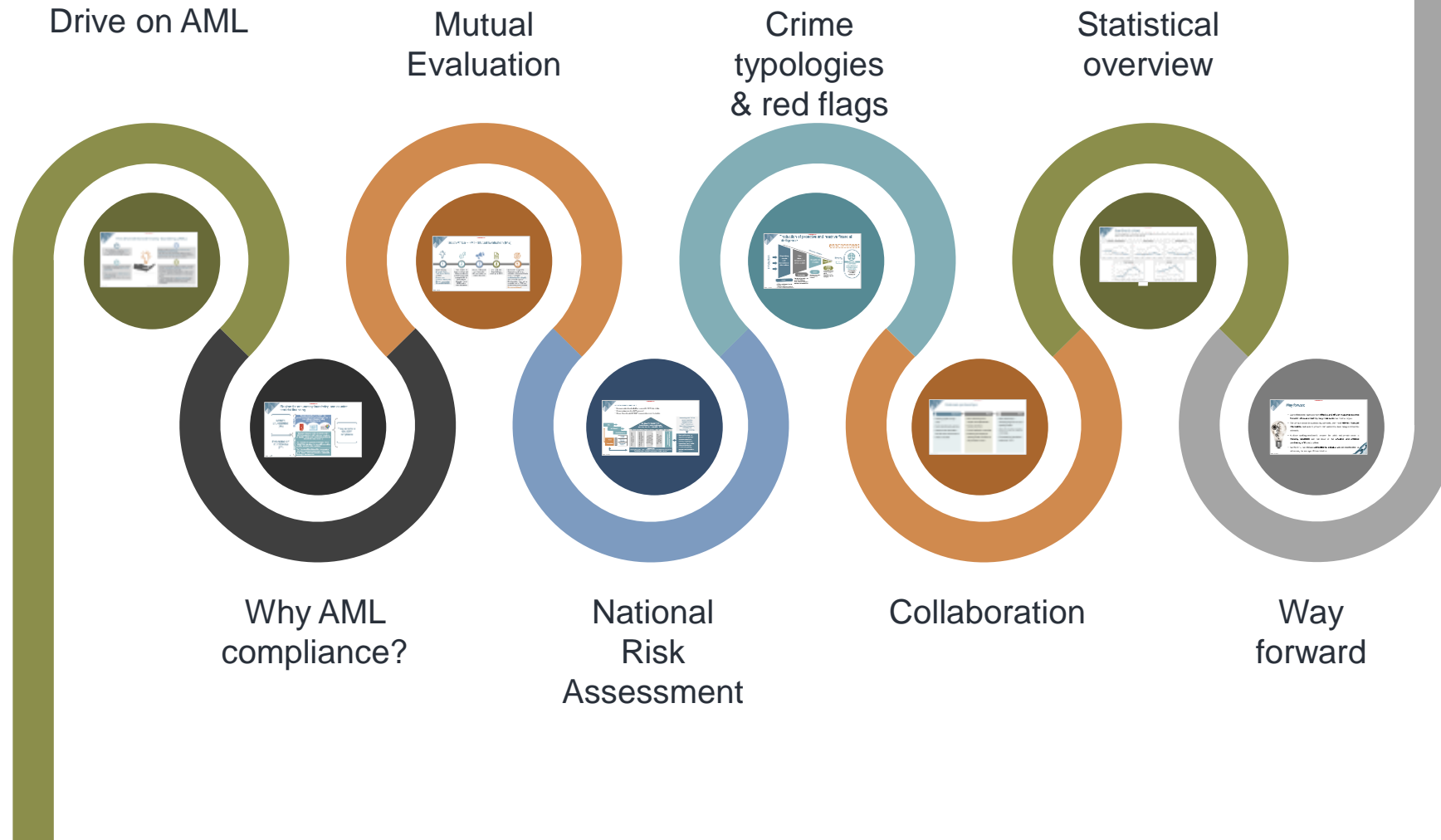
The Insurance Crime Bureau 2020 Annual Conference

Evolving financial crime typologies and
expanding possibilities for
proactive collaboration

5 March 2020

OUTLINE OF PRESENTATION

FINISH



START

The drive behind anti-money laundering (AML)

1

Drug trafficking, smuggling, **fraud**, extortion and corruption.
All illegal but also enticingly lucrative.*

2

- Proceeds from these criminal activities represent an estimated **2% to 5% of global GDP**.
- That's equivalent to **US\$800 billion to \$2 trillion** a year.
*According to the United Nations Office on Drugs and Crime.**



3

Money laundering **disguises the sources and destinations of these funds**.
This fuels some dire downstream effects, such as **compromised financial systems** and the means to keep terrorists and crime rings in business.

4

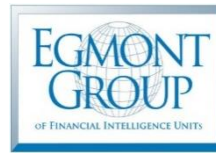
- Anti-money laundering (AML) has been a hot topic – and an **intensifying regulatory pain point** – for financial institutions for decades.
- The FATF Typologies Report (2004 - 2005) covers money laundering vulnerabilities in the insurance sector.
- The insurance sector is **rapidly expanding** and makes a substantial contribution to the market - offering sophisticated products and strong competition.

Regime for anti-money laundering and counter terrorist financing

MONEY
LAUNDERING
(ML)

GLOBAL

Financial Action Task Force (FATF) inter-governmental body focusing on combating ML and TF policy making and standards setting (IMF and World Bank)



FINANCING OF
TERRORISM
(TF)

DOMESTIC

Financial Intelligence Centre Act (Act 38 of 2001) [FIC Act] established the FIC and placed obligations on financial institutions and other businesses deemed vulnerable to money laundering.

The Prevention of Organised Crime Act (Act 121 of 1998) [POCA] introduced the crime of ML and set the penalties associated with a conviction.

The Protection of Constitutional Democracy Against Terrorist and Related Activities Act (Act 33 of 2004) [POCDATARA] introduced measures to address the financing of acts of terrorism.

7 key aspects to
AML/CFT
compliance

The FIC and why crime concerns it



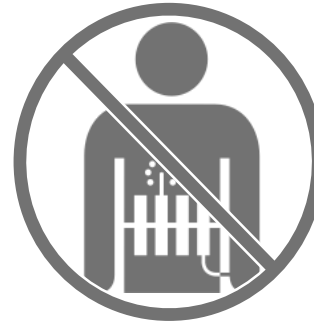
Financial
Intelligence Centre



IDENTIFY
PROCEEDS
OF
UNLAWFUL
ACTIVITIES



COMBAT
MONEY
LAUNDERING



COMBAT
TERRORIST
FINANCING

COLLABORATE AND SHARE
INFORMATION WITH:

- NPA
- LEAs
- Supervisory Bodies
- Intelligence Services
- SARS and
- Other International Agencies

SUPERVISE AND ENFORCE
compliance with the FIC Act

The FIC has **no investigative powers**, but collects, analyses and interprets financial intelligence

Business and the FIC Act

The FIC Act identifies financial and non-financial sectors vulnerable to money laundering including:



Estate agents



Banks



Long term insurers



Attorneys



Gambling sector



Motor vehicle dealers



Forex dealers

Minimum requirements from these sectors are:

Identify and
verify client
identities
(ID, KYC)
(S21)

Develop risk
management
and compliance
programme
(S42)

Keep records
of
transactions
(5 years)
(S22)

Provide ongoing
training on FIC Act
requirements to
staff
(S43)

Submit
reports to the
FIC
(STRs, CTRs
and IFTRs)
(S27, S28A,
S29, S31)

Register with
the FIC
(S43B)

Comply with the
FIC Act
- Compliance
Officer (S42A)

Risk based approach applied

Soon Crypto Asset Service providers (CASPs) will be added

Developments to FICA and regulations



International Funds Transfer Reports (IFTRs)

- Commencement of section 31 - Cross-border flow of funds (inbound and outbound, and includes CMA)
- Prescribed threshold R4 999,99.



Amendments to Schedule 1 accountable institutions

- Who is proposed to be included?
Trusts and companies' service providers, Co-operative Banks, Credit providers, Dealers in high value goods (include motor vehicle dealers, numismatic dealers, those that deal in precious metals and stones, yachts, etc.), South African Mint Company, Crypto asset service providers.
- Exit the following supervisory bodies: Estate Agency Affairs Board, Independent Regulatory Board for Auditors, National Gambling Board and Provincial Gambling Boards, and Law Societies.



Cash Threshold Reports (CTRs)

- Increased from R24 999,99 to R49 999,99.



Goal?

- Improves FIC's ability to provide **high quality information to law enforcement**
- Bring South Africa's legal framework against ML/TF in line with the **international standards** set by the FATF.

South Africa – FATF Mutual Evaluation (ME)



1

- Undertaken by Financial Action Task Force (FATF) and the
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)



2

Peer reviews of their members and SA's evaluation is part of this process during Oct 2019. International Monetary Fund (IMF) part of evaluation team



3

Issued draft report end December. SA commented by end of Jan 2020



4

2nd Draft and Face to Face meetings at FATF



5

- Final draft – Aug 2020
- Conclusions will be a reflection of how well South Africa is doing in **maintaining the integrity** of its financial system
- Final adopted report will be available on the FATF and ESAAMLG public websites
- **Follow up actions!!!**

FATF immediate outcomes (IOs)

Effectiveness ratings:

- High
- Substantial
- Moderate or
- Low level



1 | Risk, Policy and Coordination

Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.

2 | International cooperation

International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.

3 | Supervision

Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks



4 | Preventive measures

Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.

5 | Legal persons and arrangements

Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments

6 | Financial intelligence

Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.

7 | Money laundering investigation & prosecution

Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.

8 | Confiscation

Proceeds and instrumentalities of crime are confiscated.

9 | Terrorist financing investigation & prosecution

Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.



10 | Terrorist financing preventive measures & financial sanctions

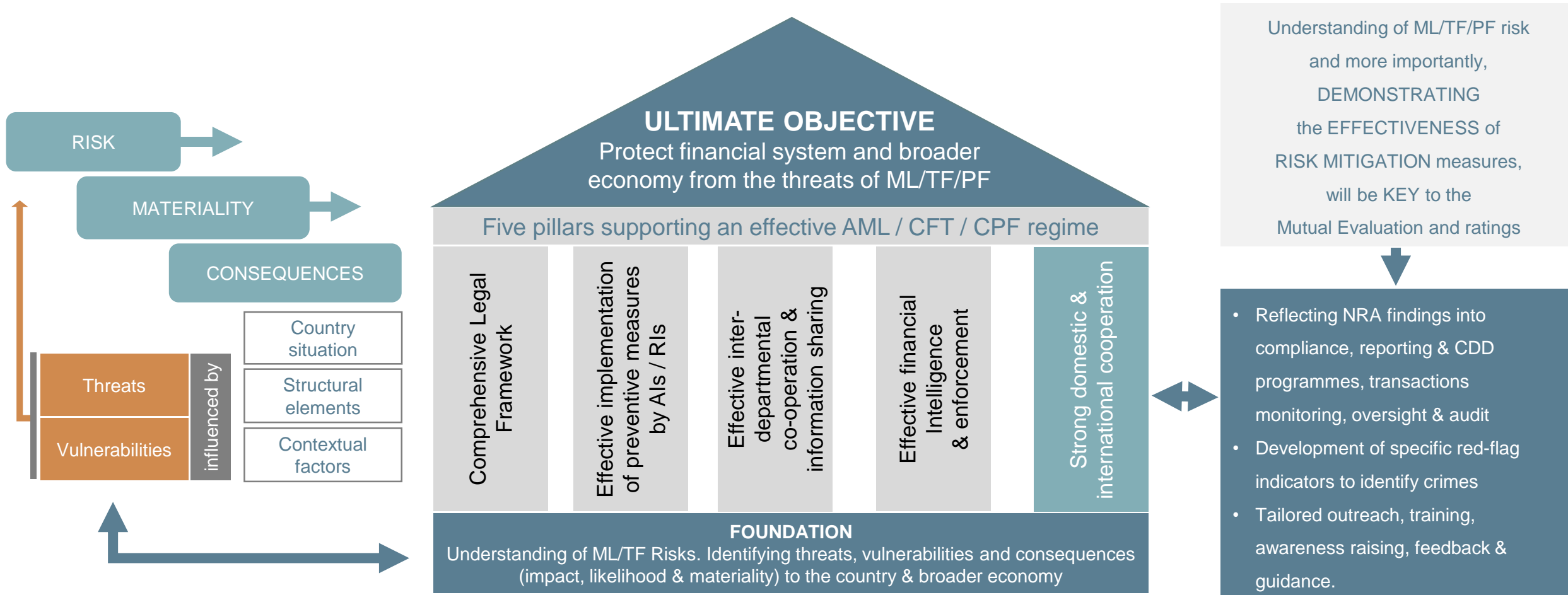
Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.

11 | Proliferation financial sanctions

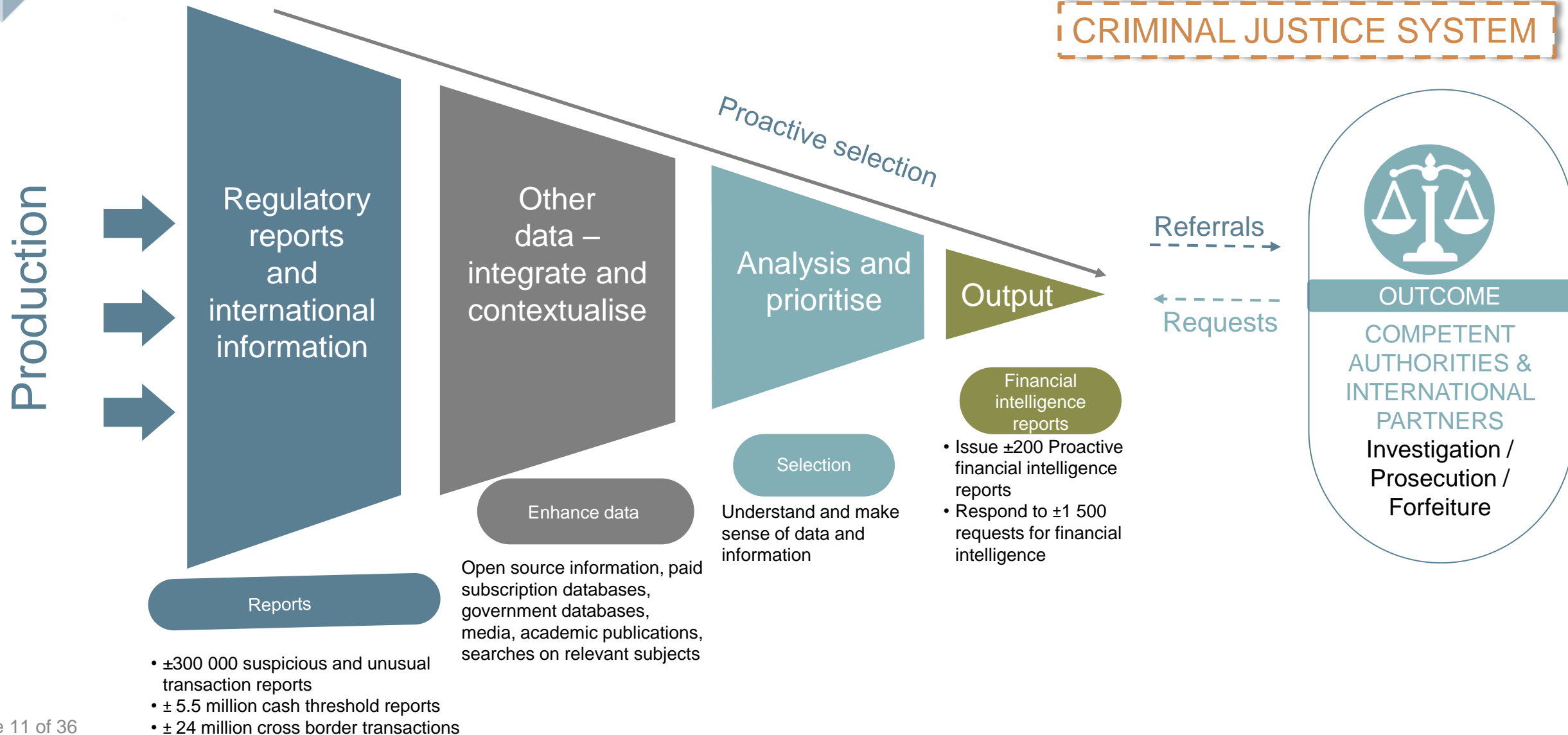
Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

SOUTH AFRICA SHOULD

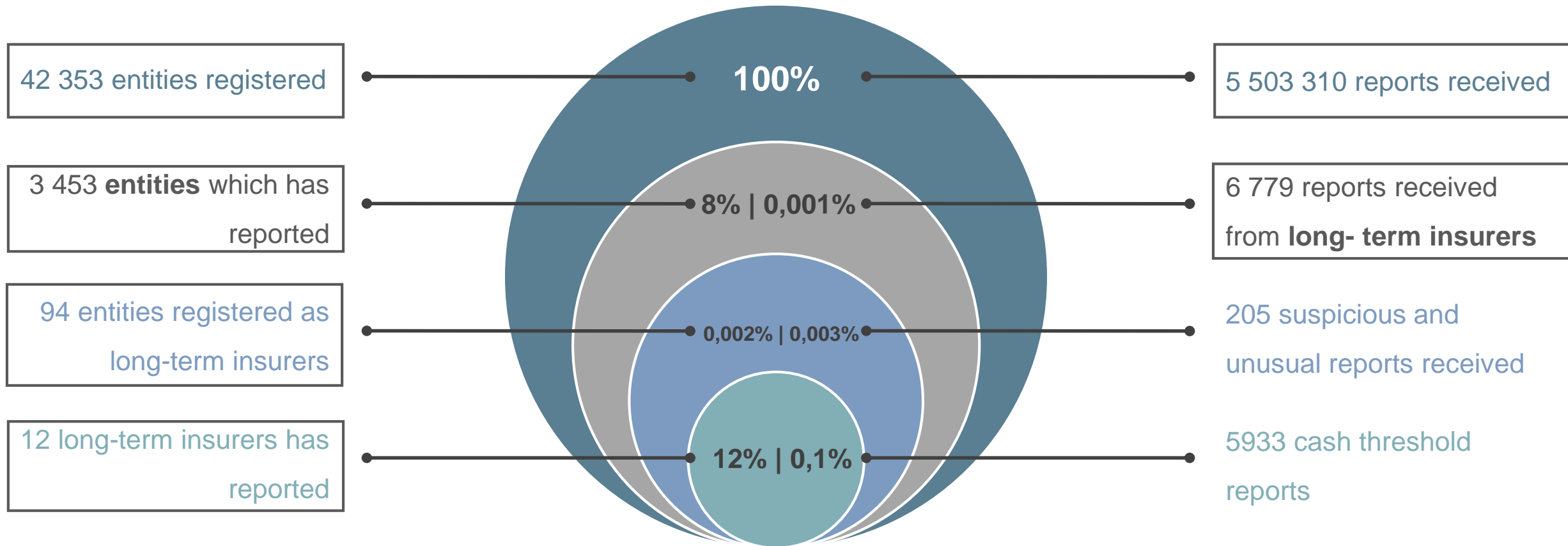
- Take appropriate steps to identify and assess ML/TF/PF risks for SA
- On an ongoing basis (keep NRA up-to-date)
- Allocate & prioritise AML/CFT/CPF resources of competent authorities



Production of proactive and reactive financial intelligence













Regulatory reporting: 1 April 2018 to 31 March 2019



Evolving payment technologies?

- Available crypto currencies: 6 624
- Crypto market capitalization: \$285.08B (Bitcoin = \$178bn)
- Top 5 according to Market Cap (as at 24 February 2020) [300k transactions daily]:

Rank	Name	Price	24h Change	7d Price Chart	24h Volume	Marketcap	Supply	Marketshare
1	 Bitcoin	\$9,810	-0.75% ↓		\$7,626,164,686	\$178,871,391,602	18,234,450 BTC	63%
2	 Ethereum	\$272	+0.52% ↑		\$6,036,759,321	\$29,823,908,989	109,829,520 ETH	10%
3	 Ripple	\$0.2758	-3.2% ↓		\$694,378,466	\$12,045,515,888	43,749,413,421 XRP	4.23%
4	 Bitcoin Cash	\$393	-0.46% ↓		\$1,076,230,323	\$7,195,787,166	18,295,663 BCH	2.52%
5	 Bitcoin Cash SV	\$291	+0.39% ↑		\$727,696,825	\$5,304,900,028	18,292,840 BSV	1.86%



- 1405. TrumpCoin (trading at \$0.0144 → +-R0.22) ????

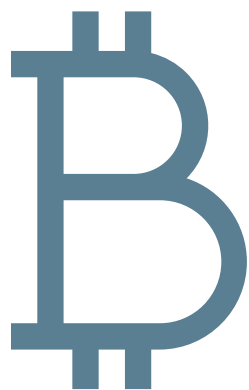
<https://www.cryptocoincharts.info/coins/info>

Challenges related to matters involving crypto currencies or assets

- **Availability** of crypto currencies (ATMs (<https://coinatmradar.com/>), exchanges, brokers, PsP trade (localbitcoins.com))
- There is no **intermediary**, "Central Bank" or "Bitcoin Office" where an investigator can check or subpoena the transactions
- **Anonymity** behind transactions - there is no "Register of Accounts" (KYC) where you can check who owns an account
- **Tracking** of crypto assets - mixer
- **Jurisdictional** and geographic limitations – will the Criminal Procedure Act of 1977 assist?
- **Expertise** – across the intelligence, investigation and criminal justice value chain including the seizing of crypto assets
- Why **Bitcoin** is relevant: 95% of law enforcement investigations dealing with crypto currencies deal with Bitcoins (Fortune magazine, 24/04/2019)



Case study 1: Money laundering through crypto currencies



- The perpetrators located in Namibia managed to **hack** into the bank accounts of two Namibian victims. The money was transferred to a fraudulently opened South African bank account in the amount of N\$750,000 and N\$500,000 respectively.
- Receiving the information from the Namibian FIC, the FIC referred the case to the AFU.
- The perpetrators created **trading accounts with Altcoin Trader**, a Virtual Currency Service Provider registered and conducting business in South Africa. Two trading accounts were created fraudulently using the credentials of two Namibian citizens.
- The money transferred to the bank account in South Africa was used to buy Bitcoin, Bitcoin Cash and Ripple **crypto currencies** on the Altcoin Trader platform. One Crypto Wallet was created for each of the accounts.
- By the time the fraud was discovered one wallet was already transferred from the Altcoin Trader platform. FIC instructed Altcoin Trader **not to proceed** with the transfer of the other wallet in terms of the FIC Act, section 34.
- AFU obtained a **preservation order** to the value of R343 000 and a forfeiture order for R 954 356 (the increase in value of the VAs over that period). An amount of R 961 654 was recovered and repatriated to the victims.



Case study 2: Cracking a Crypto currency - Ponzi Scheme

- The FIC identified what appeared to be an alleged Ponzi scheme run by an individual marketing a “**new cryptocurrency**”. This product was marketed as Africa’s first cryptocurrency and investors were promised huge returns on their investments.
- The FIC’s analysis of the individual’s bank statements revealed that there was **no cryptocurrency** and that this was indeed a Ponzi scheme.
- A restraining order was issued for more than R2.8 million in proceeds from the alleged scheme, and the FIC assisted the Asset Forfeiture Unit in obtaining a preservation order relating to **fixed property and vehicles worth more than R4 million** that was bought using the proceeds of the scheme.





Case study 4: Working with Denmark to track stolen millions

Denmark



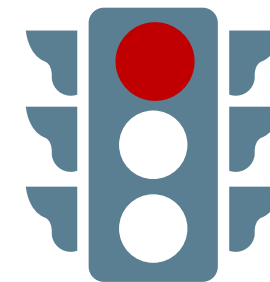
- Denmark's financial intelligence unit asked the FIC to provide information on four Danish nationals (a mother and her three adult children).
- The main subject (the mother), a former senior official was suspected of defrauding her former employer, the **Danish National Board of Social Services** of millions.
- She had been dismissed by that employer and subsequently fled to South Africa.

South Africa



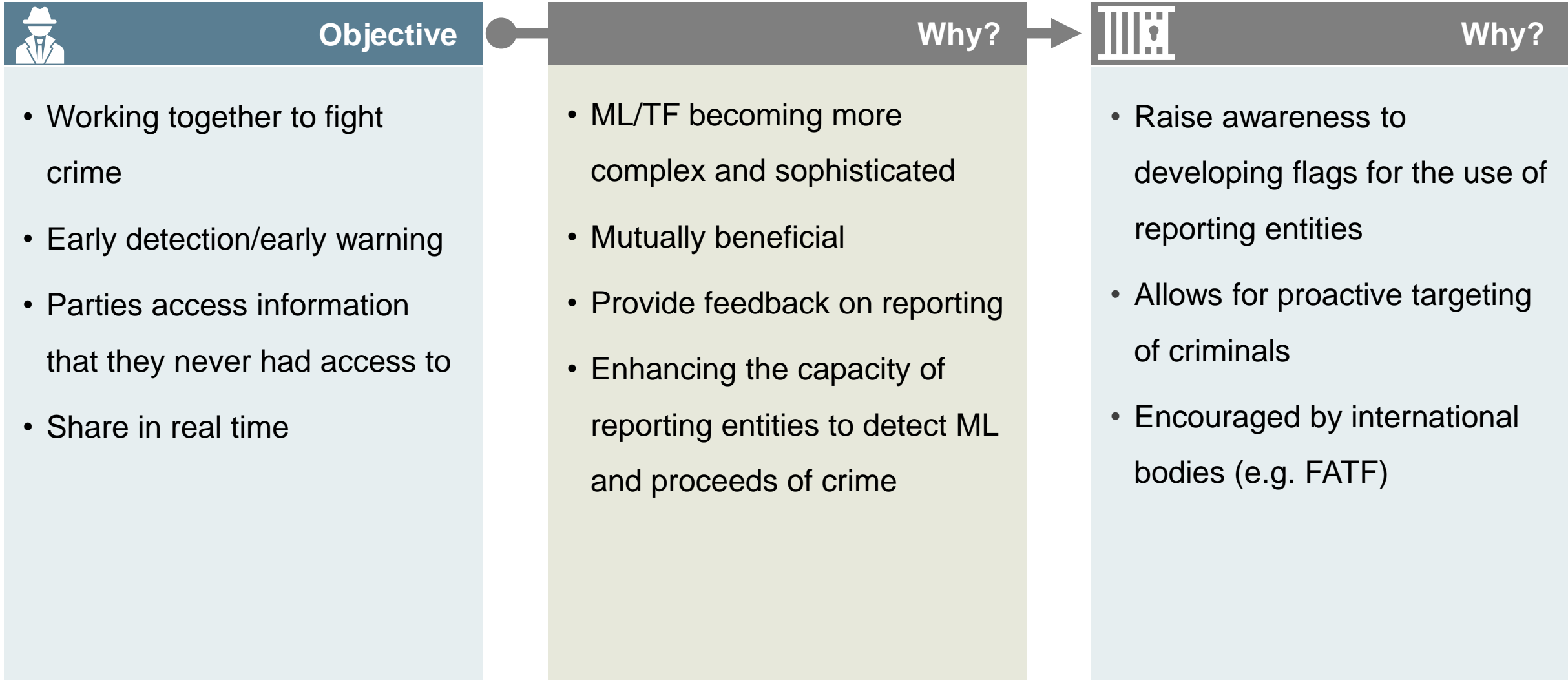
- Through its analysis the FIC identified cash and assets linked to the subject. Based on the Asset Forfeiture Unit's request, the FIC froze R6.7 million.
- The AFU has since preserved and repatriated the funds to the Danish government.

Red-flag indicators

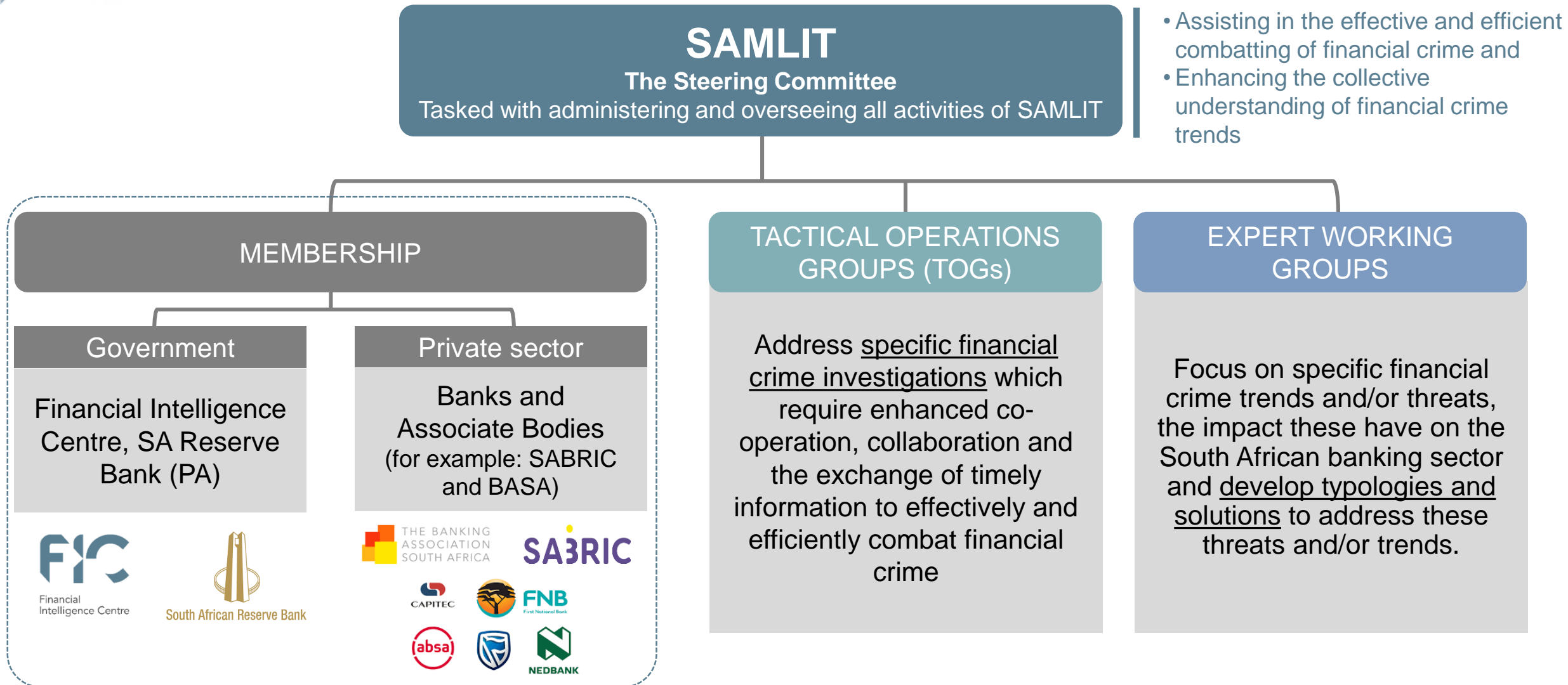


- Vehicle purchases that are seemingly not in line with the **expected income** of the customer
- Use of corporates and trusts to **layer** and hide the proceeds
- Multiple **transactions** in a short period with no underlying business rationale.
- Use of false identities and **documents**/missing documentation normally to be expected from a legitimate business
- Purchasing property in **family** members' names
- Purchasing **valuable commodities/luxury goods**, normally associated with extremely wealthy persons (Brand name boutique clothing, expensive watches and expensive electronic goods etc.).

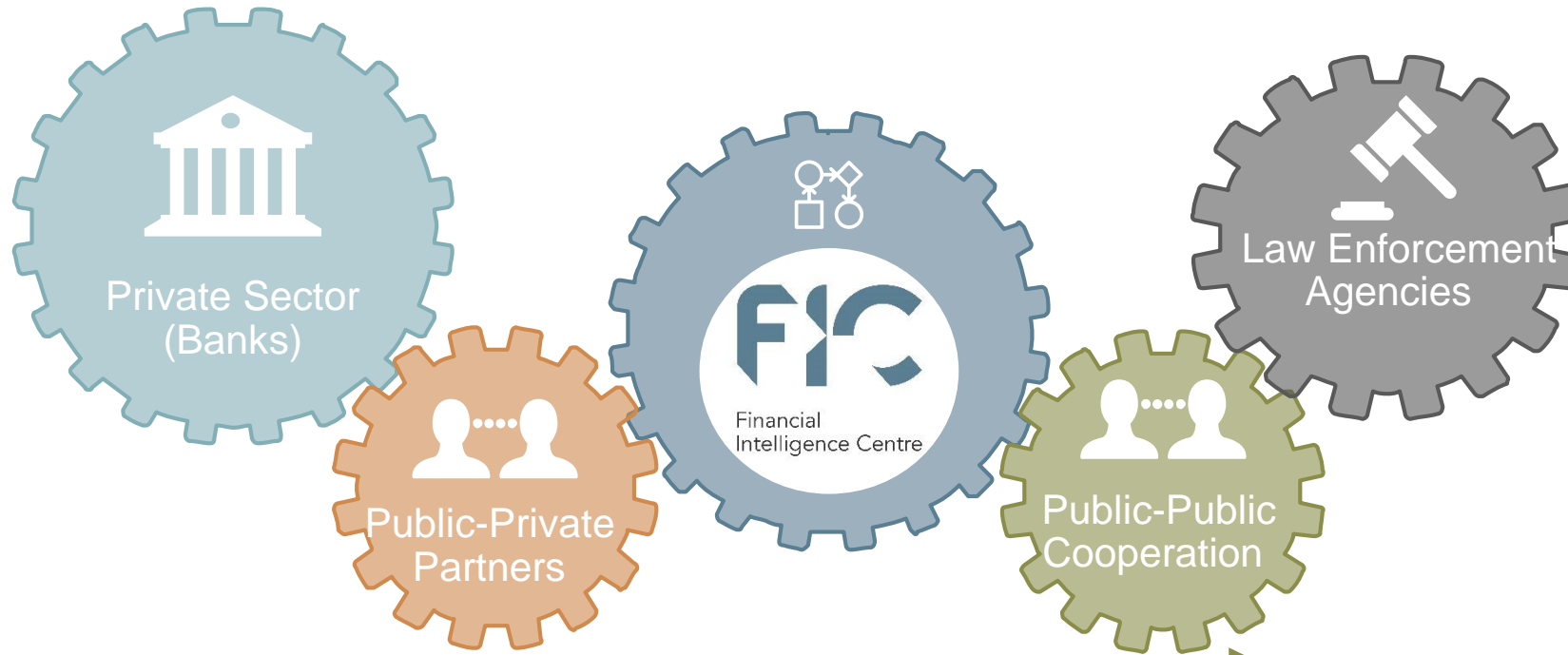
Rationale partnerships



South African Anti-Money Laundering Integrated Taskforce (SAMLIT)



Bigger picture for SA: Point of convergence – PPC and PPP



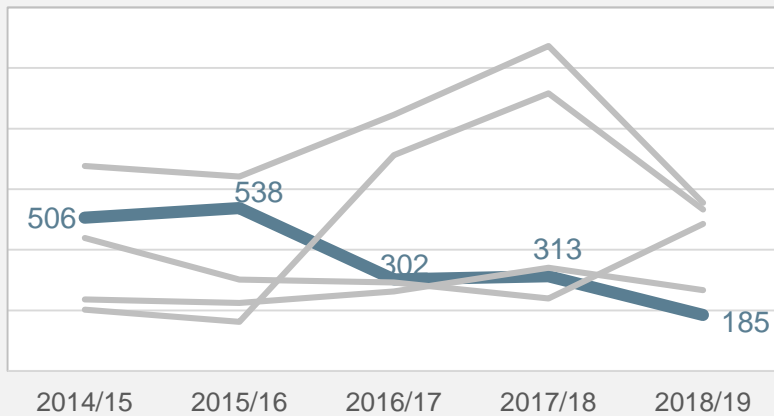
South African AML Task Force
(SAMLIT): PPP Model:
Partnership to ensure that our
financial system is intolerant to abuse

Fusion Centre: PPC Model:
Enhanced collaboration with LEA for
sharing intelligence across all levels
and sectors of government

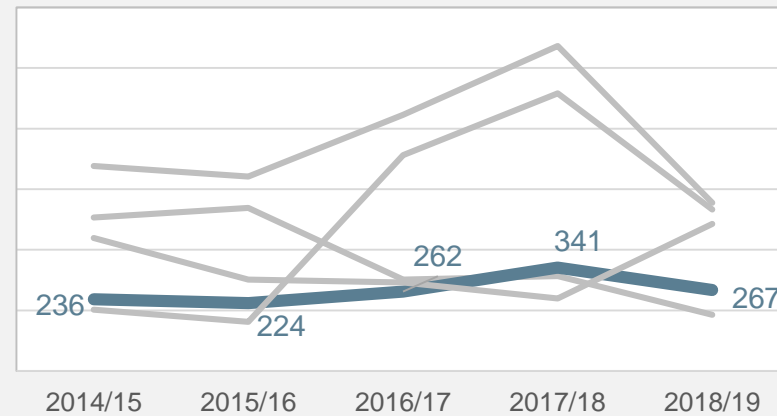
Significant crimes

Crime categories for proactive financial intelligence produced and responses to requests from law enforcement 2014/2015 to 2018/2019

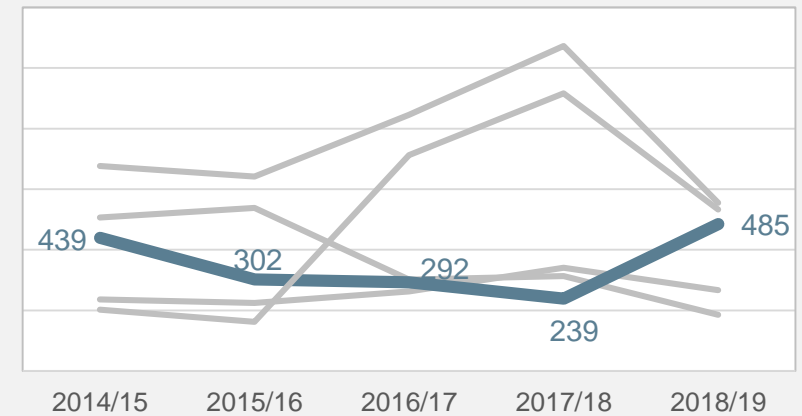
MONEY LAUNDERING



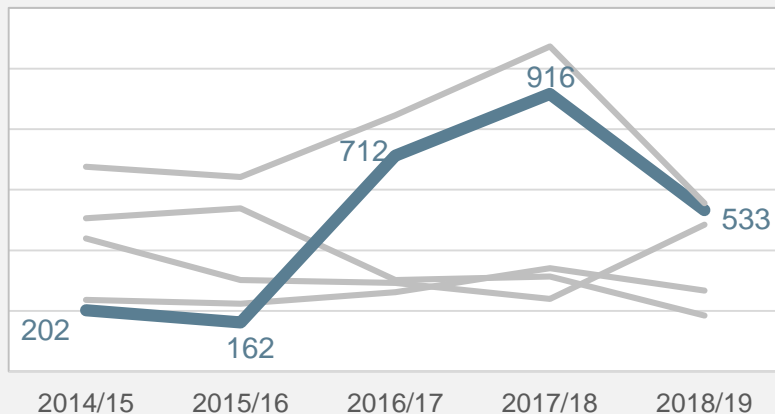
NARCOTICS



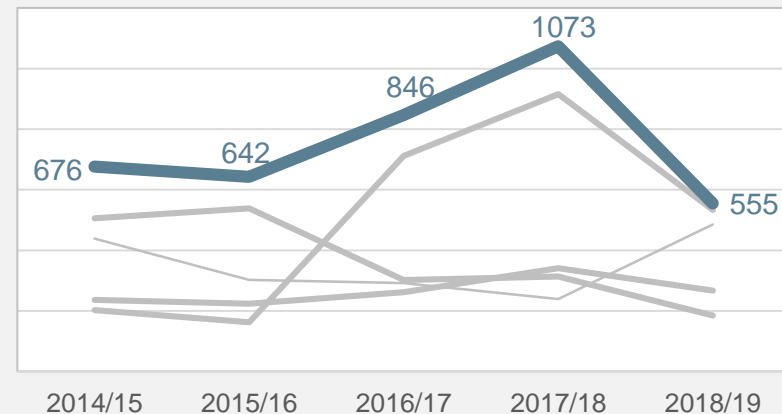
CORRUPTION



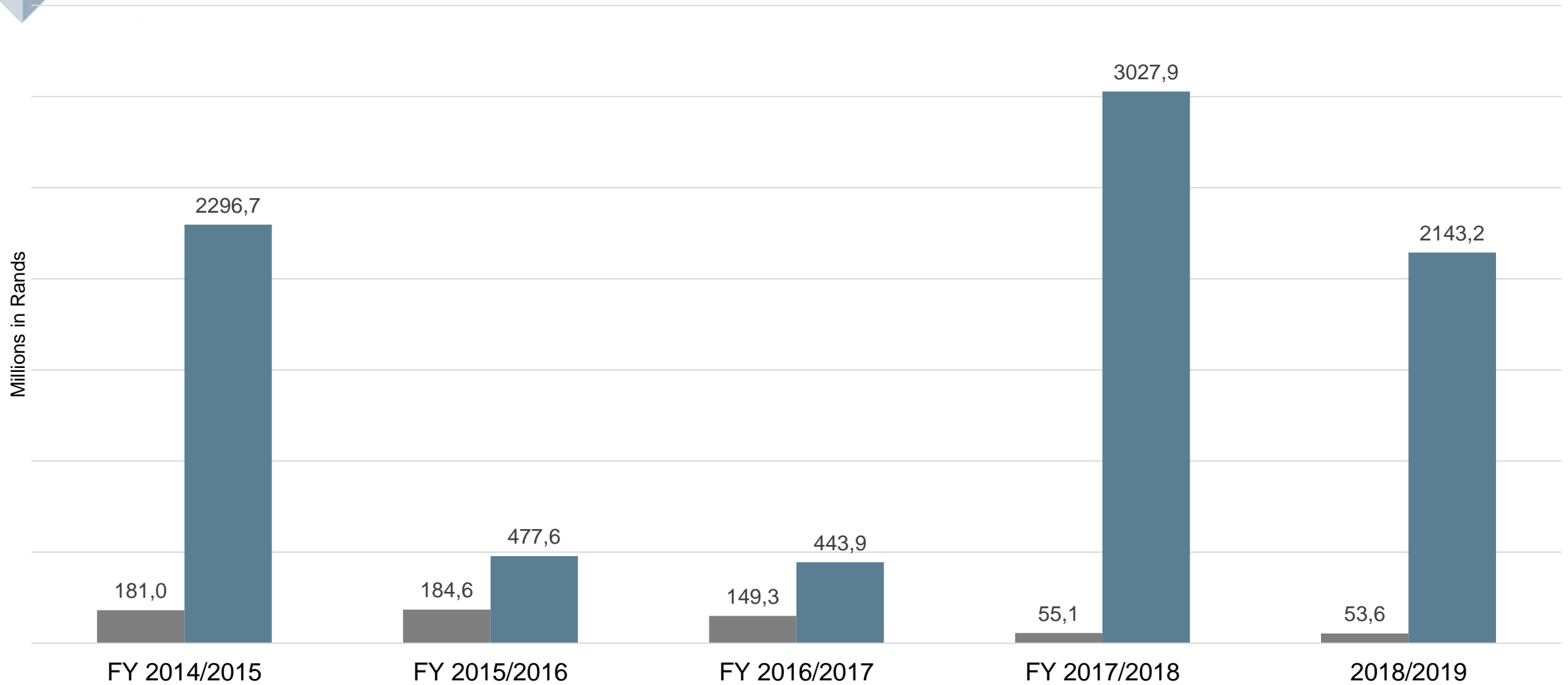
TAX CRIMES



FRAUD



Suspected proceeds of crime frozen 2014-2019



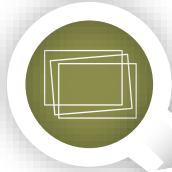
Section 34 freezing of accounts

Proceeds of crime recovered using FinInt

Analysis in figures - 2018/2019

**288 434 &
5.5mil**

Reports received –
suspicious and cash threshold



**15 663 &
15 295**

Individuals and entities
analysed



45

Bank Accounts
monitored

**39 800 &
3 382**

Enquiries with Accountable
Institutions and requests for
further information



46

Bank accounts
frozen –
R52 million



29

Affidavits
issued



R2.1billion

Contributed to the recovery



**1 054 &
1 840**

Proactive and Reactive
Intelligence Reports
produced

Typology reports

For the period **2018/2019** the FIC published the following typologies reports:

- **Case Studies and Indicators collection – Published dated October 2019**
- **Typologies and Case Studies - Published Date: March 2019**
 - Casinos and the gambling industry
 - Property sector
- **Scams and Typologies - Published Date: December 2018**
 - Scams (Crypto, Initial Coin offerings and identity fraud)
 - Typologies (PIPs, drug trafficking, rhino poaching and armed robberies)
- **Typologies - Published Date: September 2018**
 - Cybercrime, courier scams, inheritance fraud, online shopping, online gaming, crypto (Ponzi's) and fake jobs
- **Typologies - Published Date: May 2018**
 - 3rd party accounts, change of bank detail, casinos, corruption, narcotics, cybercrime, Ponzi, tax evasion and environmental crimes



Way forward

- Law enforcement agencies want **effective and efficient access to relevant financial information held by the private sector** on criminal targets.
- The private sector is exploited by criminals, they hold **relevant financial information** and seek to prevent their institutions from being exploited by criminals.
- A closer working relationship between the public and private sector is **mutually beneficial** and will result in the **effective and efficient combatting of financial crime**.
- As the FIC, we remain **committed to engage** with all stakeholders in addressing the scourge of financial crime.





Financial
Intelligence Centre

A large, abstract geometric graphic on the left side of the slide. It consists of several overlapping triangles and squares in various shades of blue and grey, creating a complex, crystalline structure.

THANK YOU