



Financial Sector
Conduct Authority

Anti-money Laundering and Counter Terrorism Financing Workshop

28 February 2019

Amendments to the FIC Act

Agenda

08:00 – 08:30	Registration	
08:30 – 08:40	Housekeeping arrangements	FSCA
08:40 – 09:15	Opening and welcome, Overview of the FSCA	FSCA
09:15 – 10:30	ML/ TF risks, RMCP, CDD	FSCA
10:30 – 11:00	Tea	FSCA
11:00 – 12:30	Record keeping, governance, inspections	FSCA
12:30 – 13:00	Lunch	
13:00 – 13:45	Registration and Reporting	FIC
13:45 – 14:45	What happens with the intelligence that is gathered?	FIC
14:45 – 15:00	Recap and closure	FSCA



What is ML/TF risks?

- ❑ Which risks are we talking about? – ML/TF risks
- ❑ ML/TF risk is the risk that your business may be used to launder money
- ❑ Money laundering and terrorism are global problems, with serious social, economic and political impact for every country in the world
- ❑ South Africa (SA) has prioritised the fight against ML/TF
- ❑ The legislative framework for combating ML/TF is:
 - POCA, 1998 – criminalises money laundering;
 - POCDATARA, 2004 – criminalises terror financing; and
 - FICA, 2001 – provides control measures to mitigate ML/TF risks.
- ❑ FIC Act was introduced to mitigate ML/TF risks





How FSPs could become vulnerable to ML/TF risks

- ❑ FSPs are constantly exposed to ML/TF risks. As the main point of contact between the public and product providers, your business can be exploited for ML/TF as follows:
 - ❑ In the **placement stage**, criminals will try to place illegally obtained money into the financial system. FSPs who collect client funds or accept cash in the business are more vulnerable. You should establish the source of funds or source of wealth
 - ❑ In the **layering stage**, criminals will attempt to break up funds, set up complex transactions and move funds around to conceal their original source and audit trail. FSPs are vulnerable because they offer many different types of financial products that could be utilised
 - ❑ In the **integration stage**, criminals withdraw funds from the financial system and use them without raising any suspicion and integrate them into the economy. By this time, the funds will appear legitimate
 - ❑ FSPs should implement measures or procedures in the FIC Act to limit the risk and protect their businesses from being abused by criminals and terrorists
 - ❑ FSPs may still be abused for ML/TF purposes despite having FICA measures in place
- 

Why was the FIC Act amended

- ❑ AML/CFT Standards have changed substantially since the enactment of the FIC Act in 2001
- ❑ Significant gaps have been identified in SA's AML/CFT regime following FATF's Mutual Evaluation in 2009
- ❑ SA was placed under constant FATF follow up process to monitor compliance and must report progress at every FATF Plenary
- ❑ After the evaluation, FATF recommendations were implemented in phases.
- ❑ The FATF findings were first addressed by amending the FIC Act in 2010.
- ❑ The FIC Act was amended again in 2017 to address most of the remaining deficiencies.
- ❑ SA has made significant progress in addressing the findings and aligning its AML/CFT legislative framework to international standards





Commencement dates of the amendments

- ❑ The FIC Amendment Act was signed into law by the President on 26 April 2017 and gazetted on 2 May 2017
- ❑ Various provisions of the Act came into effect on different dates as follows:
 - The first set of provisions commenced on 13 June 2017. These provisions did not require withdrawal or changes to existing exemptions or regulations, or systems readiness to comply with the FIC legislation
 - The second set of provisions commenced on 2 October 2017. These provisions required systems changes by accountable institutions, and the withdrawal and amendment of existing exemptions and relevant regulations
 - The last set of provisions are expected to take effect later this year. These relate to targeted sanctions - UN Security Council Resolutions





Introduction: CDD

The previous FIC Act made provision for a rule based approach for know your client (s21)

- Obtain:
 - Full names
 - Date of birth
 - ID number
 - Residential address
- Verify in the information obtained against:
 - ID Book
 - A document stating the client's residential address





Introduction: CDD

The amendments to the FIC Act now makes provision for a risk based approach for customer due diligence (s20A-21H)

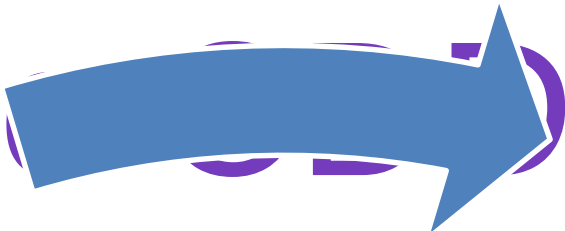
- The information that you need to obtain and verify it against depends on the institution's Risk Management and Compliance Programme RMCP.
- The contents of the RMCP is prescribed in section 42



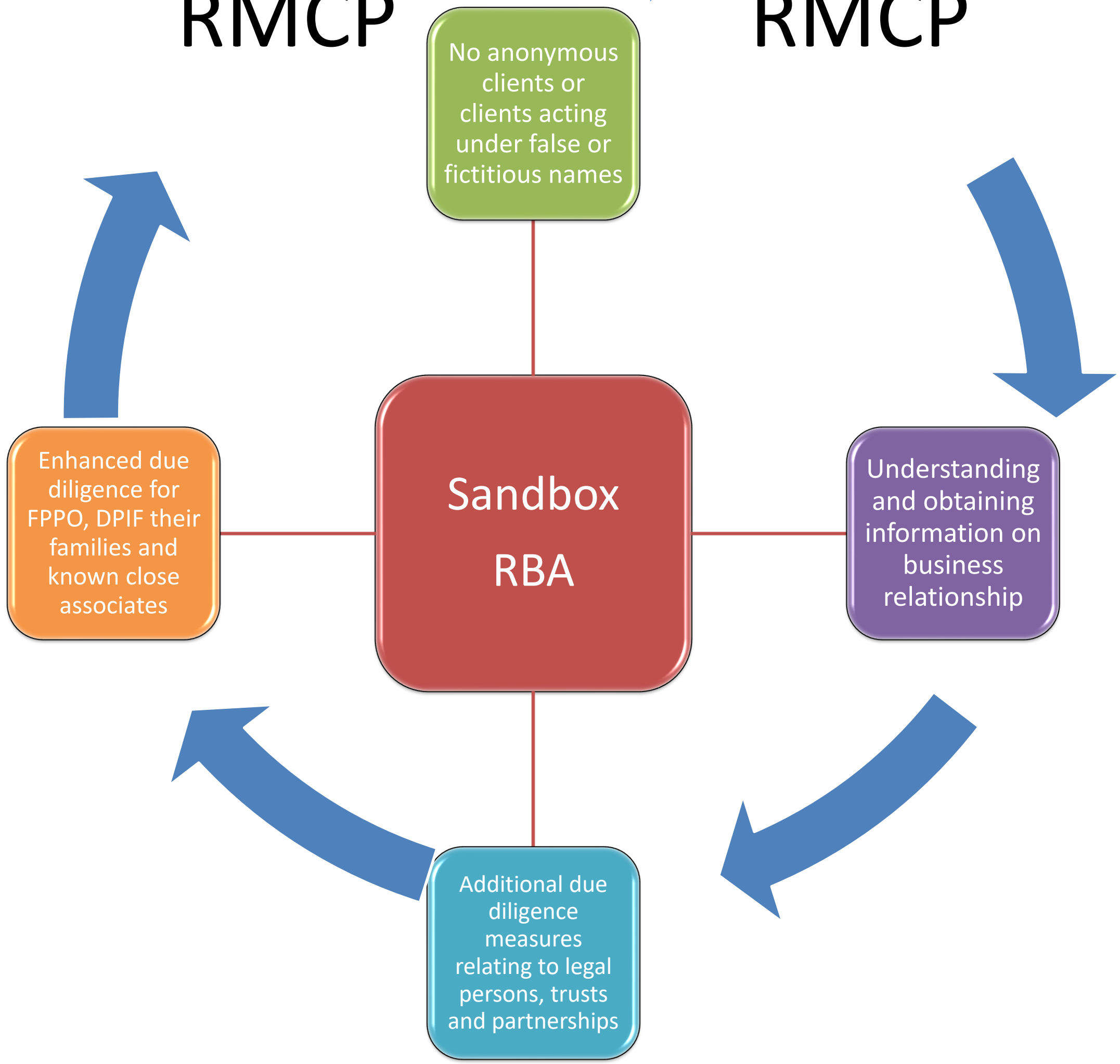


Risk Based Approach to

RMCP



RMCP



Financial Inclusion

A **single transaction** is a transaction:

- Other than a transaction concluded in the course of a business relationship; and
- The value of the transaction is less than R5 000

For a single transaction, the institution only needs to know the name of the client (s21 & s20). No verification necessary

A **business relationship** is an arrangement between a client and AI for the purpose of concluding transactions on a regular basis

The AI needs to specify in its RMCP when a client enters into a single transaction and when it is establishing a business relationship (s42(2)(b))



Business relationship

In addition to CDD the AI needs to obtain information from the client to enable it to determine whether future transaction are consistent with the institution's knowledge of the prospective client, including information describing:

- The nature of the business relationship concerned;
- The intended purpose of the business relationship concerned; and
- The source of funds which the prospective client expects to use in concluding transactions in the course of the business relationship





Customer due diligence

- AI's now have the flexibility to choose the type of information by means of which it will establish clients' identities and also the means of verification of clients' identities, instead of following the rigid steps provided for in the MLTFC Regulations.
- An AI should always have grounds on which it can base its justification for a decision that the appropriate balance was struck in a given circumstance.
- The systems and controls by which an institution decides to manage ML/TF risks and the levels of due diligence it chooses to apply in relation to various risk levels must be documented in its RMCP.



Customer due diligence

Enhanced due diligence

High Risk Client

More information obtained from client

More secure confirmation of clients' information

Closer scrutiny of clients transactions

Low Risk Client

Less information obtained from client

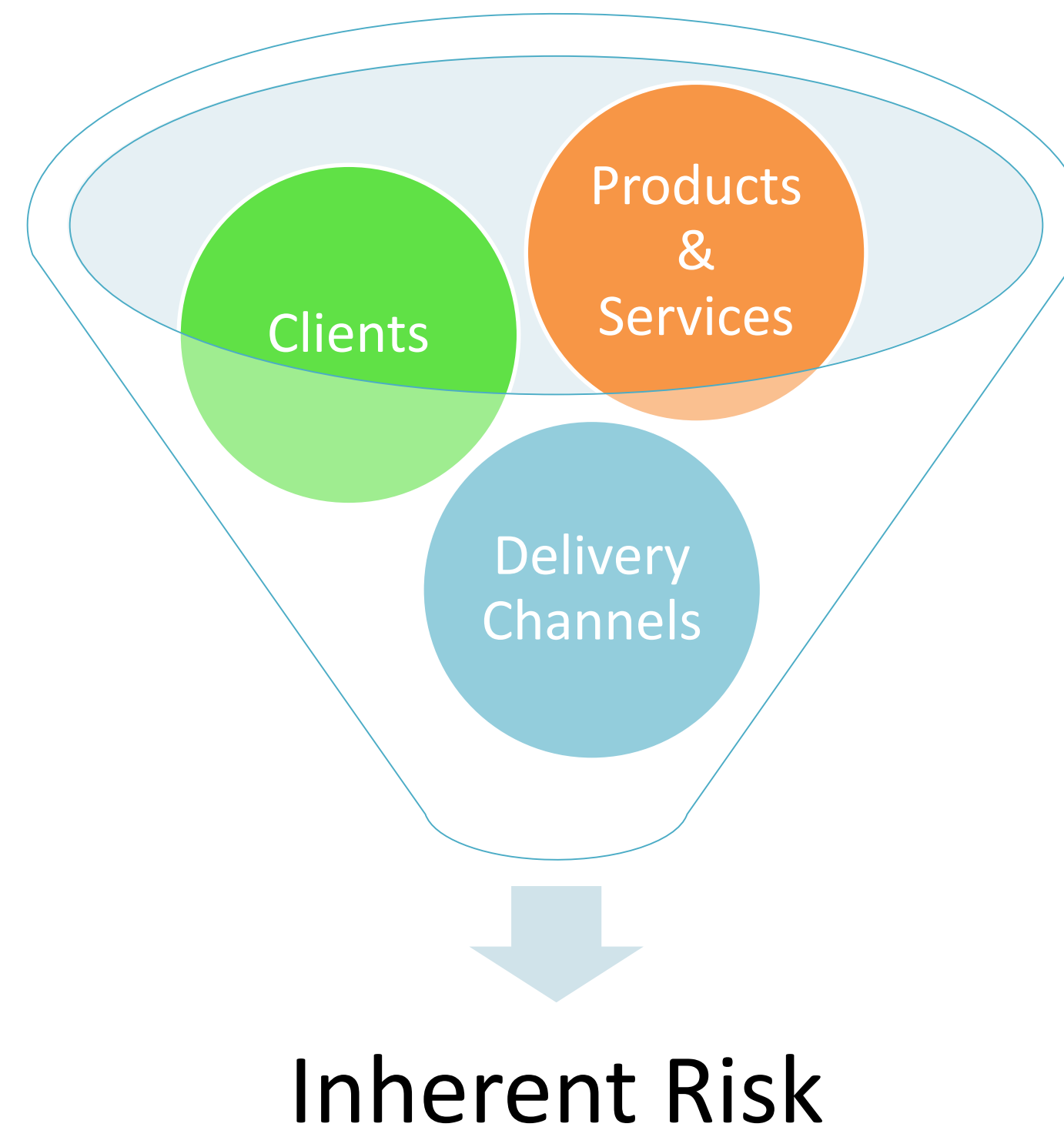
Less secure confirmation of clients' information

Less frequent scrutiny of clients transactions

Simplified due diligence

Risk Evaluation

Factors that may be indicative of ML/TF risks relate to a number of aspects such as product or service features, delivery channels, geographic areas, etc. and each of these may interact differently with the characteristics of different types of clients.



Natural Persons

- At the very basic level the following information needs to be obtained:
 - person's full names;
 - date of birth;
 - a unique identifying number issued by a government source
- This may be supplemented by applying other attributes of a natural person including:
 - his/her physical appearance or other biometric information;
 - place of birth;
 - family circumstances;
 - place of employment or business;
 - residential address;
 - contact particulars (e.g. telephone numbers, e-mail addresses, social media);
 - contacts with the authorities (e.g. tax numbers) or with other accountable institutions.
- This list of examples is not exhaustive and depends on the risk profile of the client



Natural Persons

- Verification methods vary. Regardless of the method applied, it is important that verification be done using information obtained from a reliable and independent third-party source and, as far as possible, the original source of the information.
- AI's should, as far as practicable, use government issued or controlled sources as the means of verification when verifying basic identity attributes:
 - ID or smart card
 - Valid driver's license
 - Foreign identity documents
 - Passports
 - Asylum seeker or refugee permits
 - Work permits
 - Visitor's visas
- The Centre encourages AI's to make use of information in electronic form to corroborate a prospective client's information against multiple third party data sources.



Ongoing due diligence

- Scrutiny of transactions undertaken throughout the business relationship including:
 - The source of funds to ensure transactions are consistent with knowledge of the client and client's business and risk profile
 - Pay attention to unusual patterns of transactions or unusually large or complex transactions
- Ensure client information is accurate and relevant
- Frequency and intensity of ongoing due diligence based on money laundering or terror financing risks associated with business relationship with client
- Ongoing due diligence processes detailed in risk management and compliance programme



Inability to conduct due diligence

- Prohibits AI from entering into or maintaining business relationship or concluding single transaction if it cannot perform customer due diligence
- Consider report in terms of section 29
- Risk management and compliance programme should indicate the sequence of attempts to obtain the required information as well as when verification must be completed and at which point the conclusion is reached that the information is not forthcoming and is therefore unable to conduct customer due diligence
- Risk management and compliance programme should also provide for the manner in which it will terminate an existing business relationship when unable to complete customer due diligence requirements



Foreign prominent public official

- AI must know who their clients are and understand their client's business
- Business with foreign prominent public officials must always be considered high risk
- AI must
 - Obtain senior management approval for establishing the business relationship
 - Take reasonable measures to establish the source of wealth and source of funds of the clients; and
 - Conduct ongoing monitoring of the business relationship
- Examples:
 - Head of State, or head of a country or government
 - Member of a foreign royal family
 - Government minister or equivalent senior politician or leader of a political party
 - Senior judicial official
 - Senior executive of a state owned corporation
 - High ranking member of the military

Domestic prominent influential person

- AI must know who their clients are and understand their client's business
- Business with domestic prominent influential persons is not always considered high risk
- AIs will have to include the management of business relations with person in prominent positions in their risk management and compliance programme

Public functions	Private functions
President, Deputy president	Chairperson of board of directors, chairperson of audit committee, EO, CFO of company that provides goods or services to the State and annual transactional value exceeds the amount determined by the Minister
Minister, Deputy Minister	
Premier, member of executive council	
Mayor	
Leader of a political party	
Member of the royal family	Head or executive accountable to the head of international organisation based in RSA
Accounting authority, CFO of a public entity listed in PFMA	

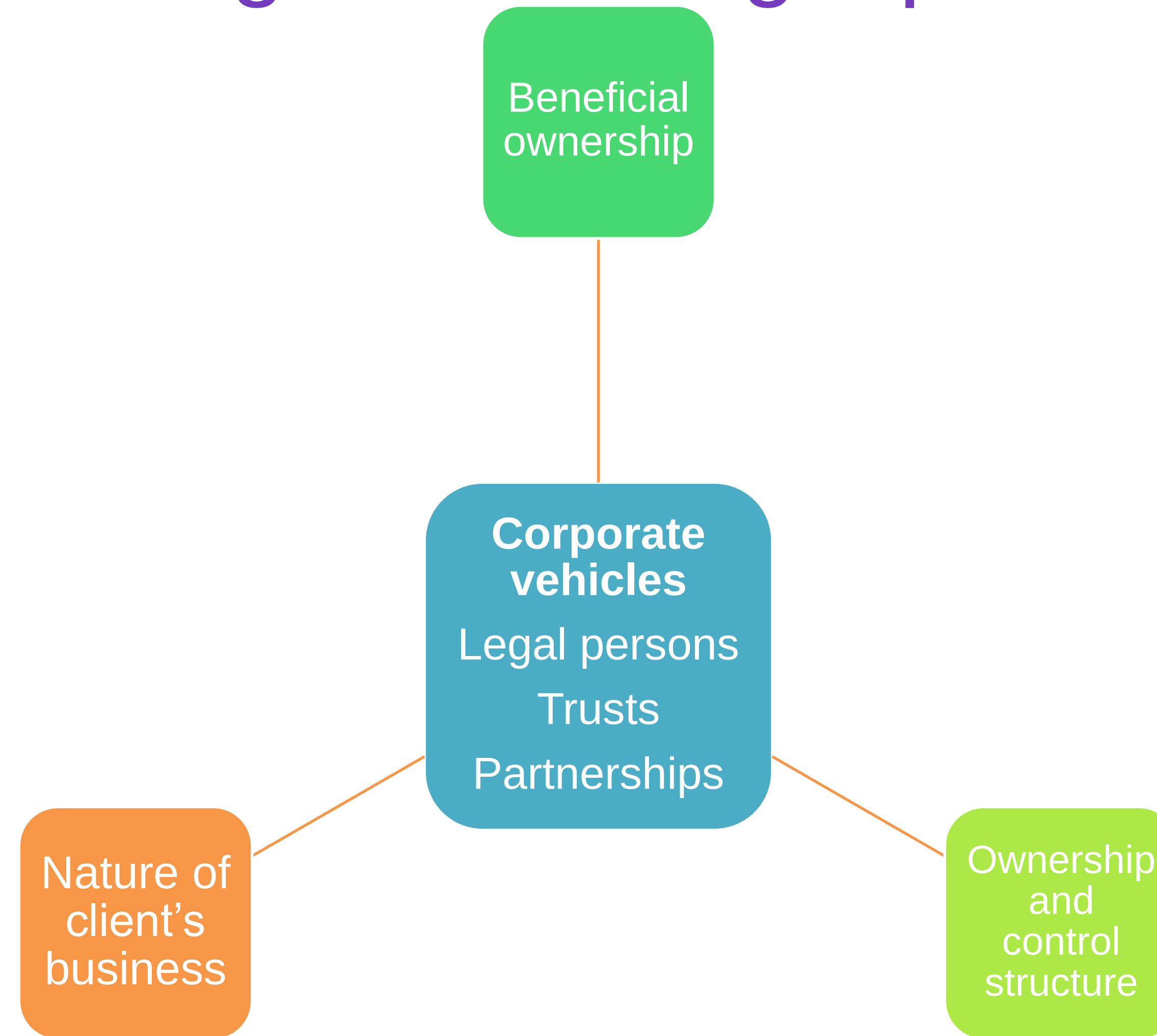


Family members and known close associates

- The provisions on foreign prominent public officials and domestic prominent influential persons also applies to their immediate family members and known close associates
 - Current or previous spouse, civil partner or life partner
 - Children and step children and their spouse, civil partner or life partner
 - Parents; and
 - Siblings and step siblings and their spouse, civil partner or life partner



Additional due diligence for legal persons, trusts and partnerships



Legal persons

Definition

A legal person is defined in the FIC Act as any person, other than a natural person that establishes a business relationship or enters into a single transaction with an AI table institution and includes:

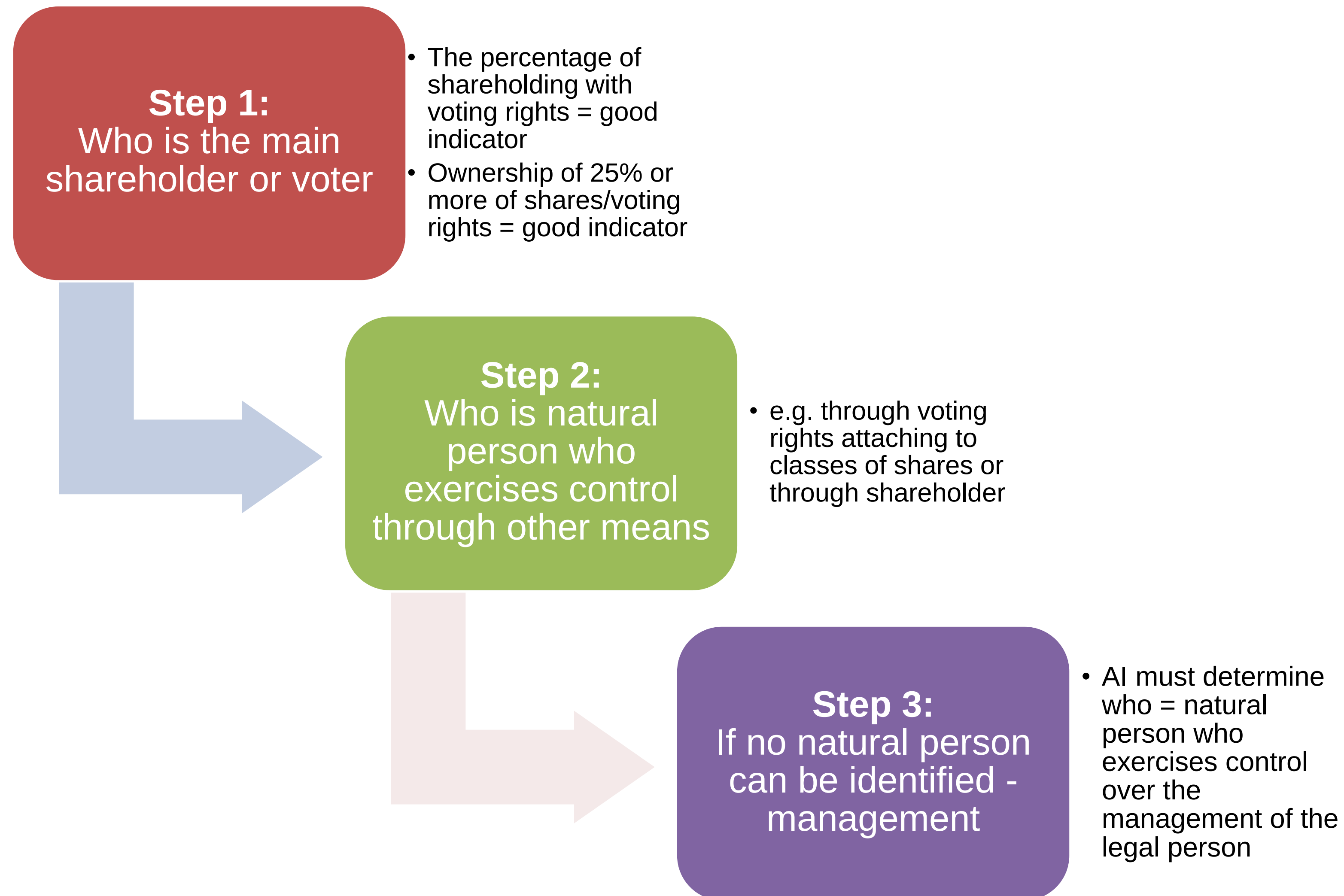
- A person incorporated as a company
- Close corporation
- Foreign company
- Or any other form of corporate arrangement or association but **excludes** a trust, partnership or sole proprietor.



Legal persons

Characteristics which describes identity of legal person	Verification
Name and trading name	AI to decide on degree and methods of verification based on money laundering or terror financing risk
Form	
Registration number	Methods may vary
Address of registered office/business address if different	Verification with information obtained from a reliable and independent third-party source
Powers	
Directors	
Senior management	As far as possible the original source of the information
Tax numbers	

Legal persons: Beneficial ownership





Partnerships: Beneficial ownership

Identify	Verify
Name of the partnership	Take reasonable steps to verify particulars AI needs to be satisfied that it knows the identities of natural persons concerned
Identity of each partner	
Person who exercises control over partnership	
Person who is authorised to enter into business relationship or single transaction	



Trusts: Beneficial ownership

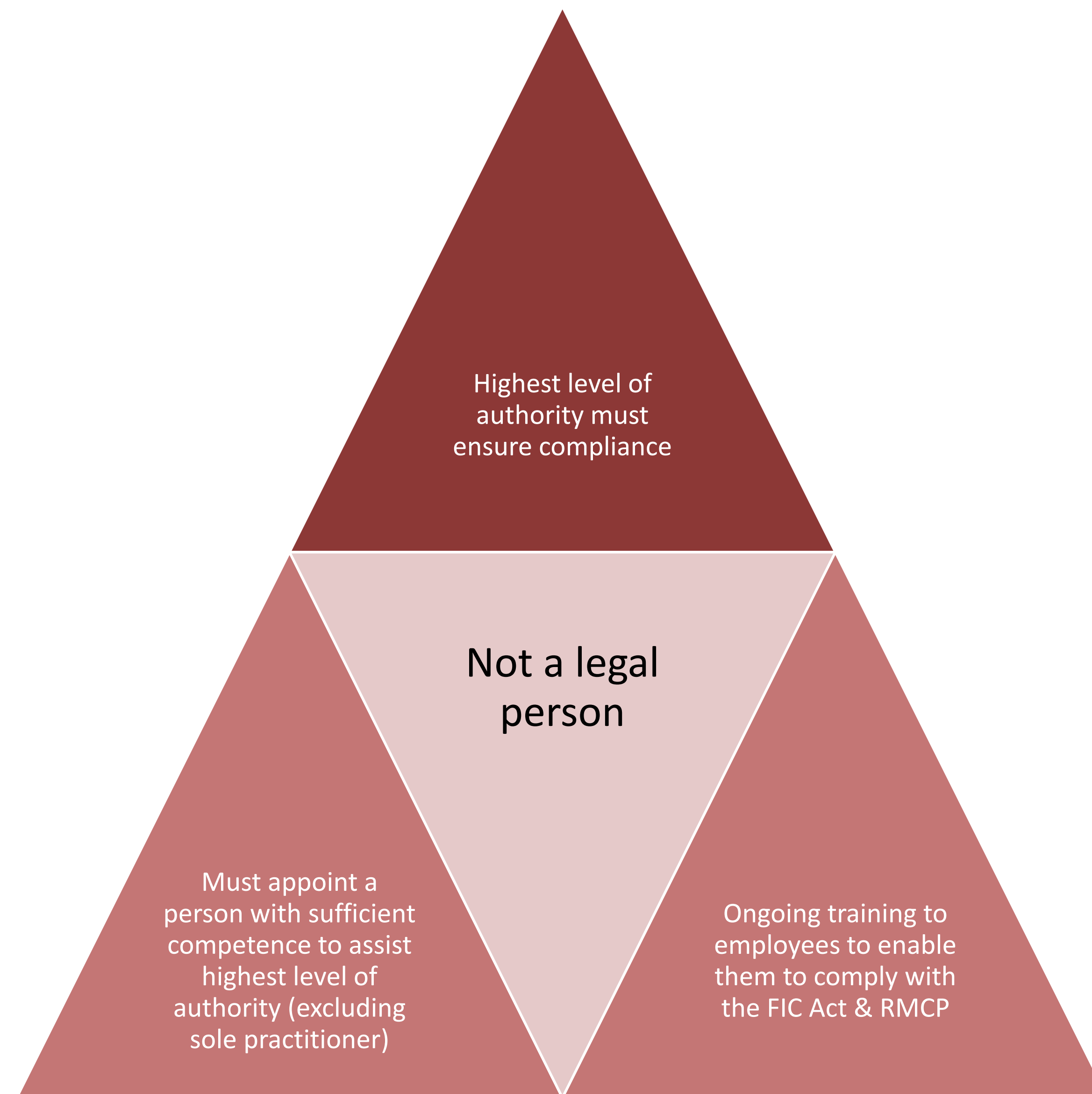
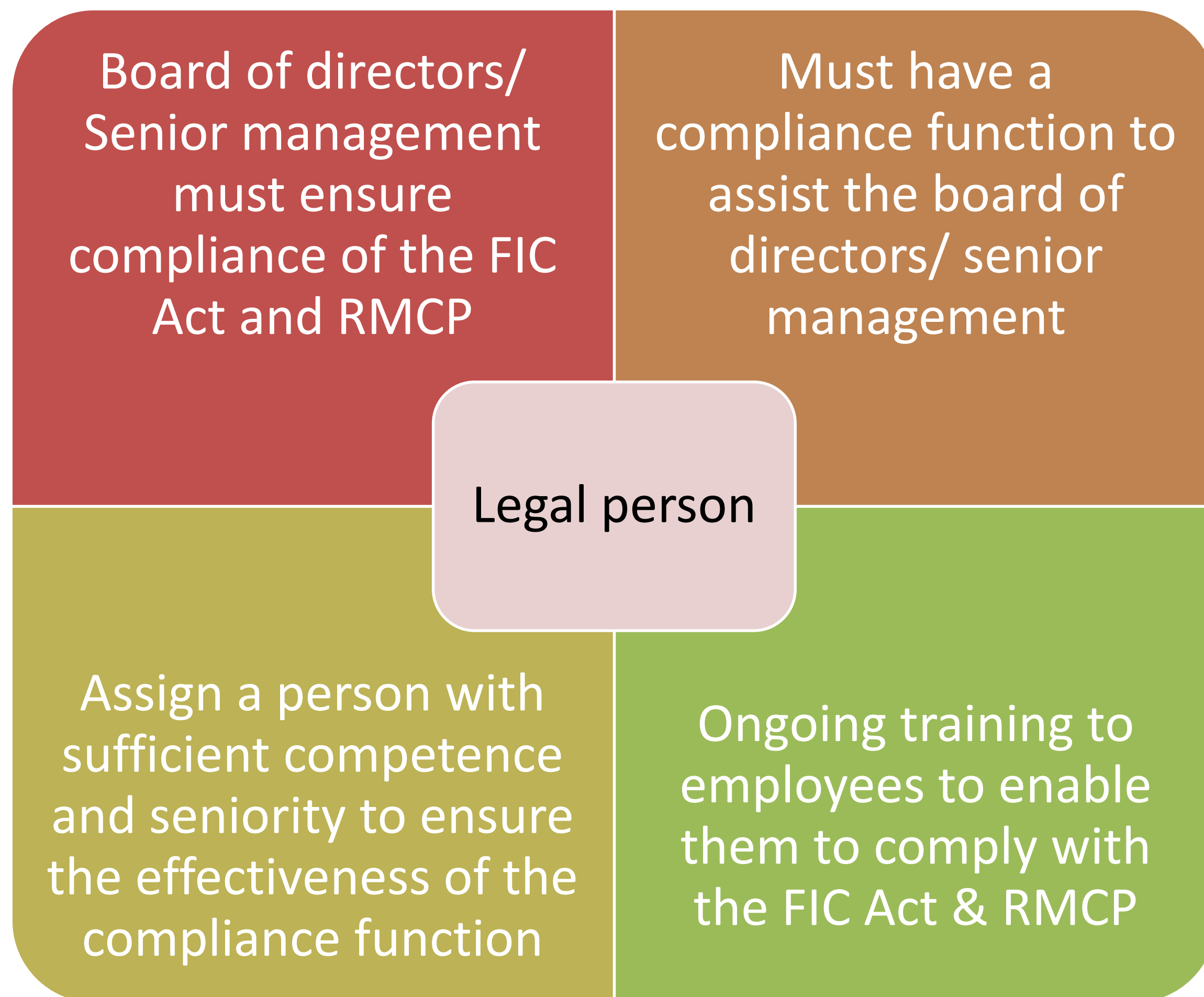
Identify	Verify
Name and number of trust	Take reasonable steps to verify
Address of the Master where trust is registered	
Identity of founder	AI needs to be satisfied that it knows the identities of natural persons concerned
Identity of each trustee	
Person who is authorised to enter into business relationship or single transaction	
Identity of each beneficiary or how they will be determined	



Record keeping

- Records must be kept of CDD information for 5 years
- Record must be kept for 5 years of every transaction that are reasonably necessary to enable that transaction to be readily constructed and must include:
 - Amount involved
 - Date transaction concluded
 - Parties to the transaction
 - Nature of the transaction
 - Business correspondence
 - Account facilities of the client
- Record must also be kept of transactions or activity which gave rise to a STR or SAR for 5 years from the date on which the report was submitted to the FIC
- Records may be kept by third parties as long as the AI has free and easy access to the records and the records are readily accessible to the FIC and FSCA
- Records may be kept in electronic form and must be capable of being reproduced in a legible format

Governance



Transactions reported during 2017/18

Accountable Institution	CTRs	STRs	TPRs	Percentage of total reports
Authorised users of an exchange	31 498	127	0	0,6%
Collective investment schemes	860	64	0	0,02%
Long term insurers	1757	110	0	0,04%
Investment advisors and intermediaries	26 462	1 164	0	0,5%





Common inspection findings

1. Customer due diligence not understood and applied correctly
2. Cash threshold transactions not reported or reported late
 - Dual reporting
 - Cash threshold report aggregation
3. Suspicious or unusual transactions not reported or reported late
4. Risk management and compliance programme not developed, not understood or incorrectly implemented
5. No employee training or training provided is superficial, sporadic and incomplete
6. Compliance not a board or senior management responsibility
7. Compliance officer not of sufficient competence or seniority
8. Failure to register or late registration
9. Failure to comply with Directive 4 – update registration details and activate profile on goAML





Scope of inspections

Compliance duty		Section	Regulation		Directives, Guidance notes & PCCs		Administrative sanction	Criminal sanction
Customer due diligence		20A-21H	1A		GN7		Natural Person = R10 million Legal Person = R50 million except STR	Not criminalised
Record Keeping		22-24	20		PCC2			
Reporting	CTR	28	22, 24	22B-22C	Dir 3	GN5B		15 years imprisonment or R100 million fine
	TPR	28A		22A, 23B, 23C		GN6		
	STR	29		23-23A		GN4A		
Governance	RMCP	42			GN7			
	Accountability	42A			GN7			
	Registration	43B	27A		Dir2, PCC5C			
	Training	43			GN7, PCC18			

THANK YOU