



Financial  
Intelligence Centre

# Risk-based approach and the risk management and compliance programme

Presented by Ashleigh Mooij  
11 September 2018

# SCOPE

## Risk-based approach

- What is risk
- What is required of an accountable institution in terms of the risk-based approach?

## Unpacking the risk management and compliance programme

# Risk-based approach

- Amendments to FIC Act resulted in paradigm shift

## Rules based “old”

- Prescriptive
- Narrow/strict interpretation of requirements
- Minimal ownership of AML understanding by AIs
- Tick box approach applied

## Risk based “new”

- Risk to AI is fundamental in application
- Ownership in understanding AML risk
- Focus on higher risk areas
- Compliance requirements met more efficiently and cost effectively



# Risk-based approach

## What is risk?

- Likelihood and impact of uncertain events on set objectives.

*International best practice rating methodology*

- Uncertainty is a function of
  - Threats – potential to cause harm
  - Vulnerability – things that can be exploited by threats
  - Consequence – impact of threat/exploitation

# Risk-based approach

- Which risks are we talking about?
- Money Laundering risk

## Money Laundering

- Proceeds of crime
- Placement, layering, integration
- Proceeds no longer associated with underlying criminal activity
- Proceeds appear legitimate

### STAGES OF MONEY LAUNDERING

#### — 1 — PLACEMENT

Criminals deposit illicit money into bank accounts

Buy high-end goods with illicit cash

Break up large amounts of illicit cash & deposit it into smaller amounts over time

Gamble with proceeds

Think of a HOT potato... It (funds) needs to be put down (placed) so you don't burn your hands



#### — 2 — LAYERING

Criminals need to create distance between proceeds of crime & those involved in the source of proceeds

Buy & resell high-end goods

Buy bonds, invest in legitimate businesses, invest in property

The HOT potato (funds) is thrown from person to person (distancing yourself from it)



#### — 3 — INTEGRATION

Proceeds are now fully part of the financial system

Criminals are free to buy more luxury items and deepen the spread of proceeds

Criminals may look to grow proceeds seeking legitimate or illegal investment opportunities

The HOT potato (funds) is now cooled (funds laundered) and criminals can enjoy their proceeds



# Risk-based approach

- Terrorist financing risk

## Terrorist Financing

- Solicitation, collection and providing funds and assets with intention to be used to support terrorist acts, terrorist organisations and individual terrorists
- Illegal and legal sources
- Goal – to conceal financing and nature of activity being financed



# Risk-based approach

## Unpacking money laundering and terror financing risks

- These are **threats** and **vulnerabilities** which put accountable institutions at risk of being **abused** in order to facilitate money laundering and terror financing activities
- Potential that clients may **use products and services** offered by the accountable institution for money laundering and terror financing purposes
  - Launder proceeds
  - Blur detection, investigation or prosecution of money laundering
- Applying a risk-based approach ensures that AIs are able to ensure that **measures** to prevent money laundering and terror financing **are in proportion** with the **risks** identified

# Risk-based approach – risk management



- Identification of risk



- Assess the risk



- Methods to manage the risk



# Risk-based approach

## • Identification of risk

### Factors to take into account when identifying risks

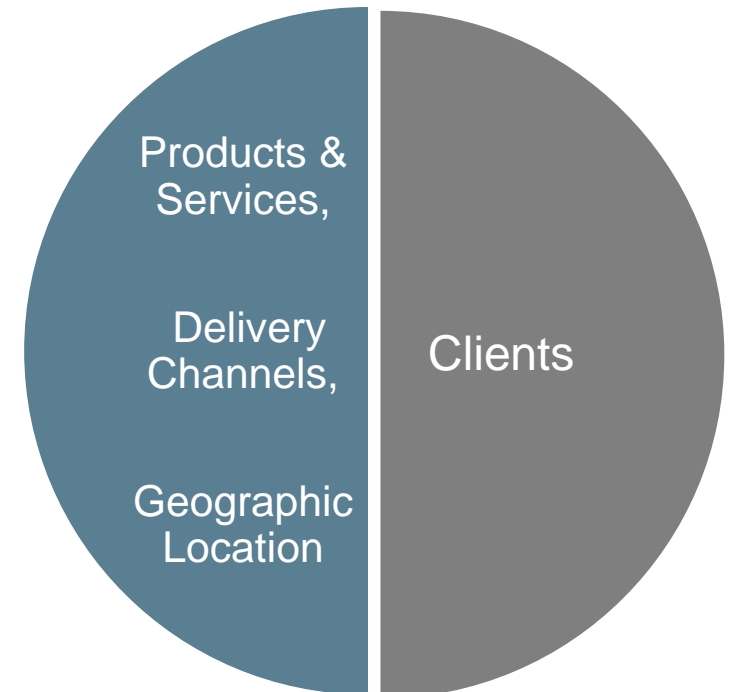
- Products and services
- Delivery channels
- Geographic location
- Clients
- Other factors



# Risk-based approach

- **Assessment of risk**

- Review of the identified risk, applicable indicators and the interaction with different types of clients
- Understand the impact of the indicators



# Risk-based approach



- **Assessment of risk**

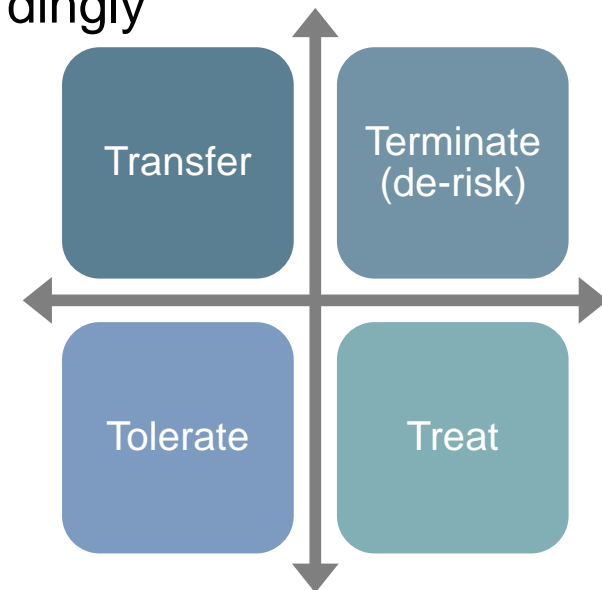
- Risk rating, by assigning categories to different levels of risk
  - High/Medium/Low risk
- No “one size fits all” approach
- Risk rating may change, re-evaluation of risk rating is critical
- Smaller AI’s – simplistic risk scale
- Complex structures with multiple indicators – more sophisticated risk scale

# Risk-based approach

## • Methods to manage risk

### Treating the risk

- Risk mitigation – entails control measures, systems and minimising the money laundering and terror financing risk
- Align money laundering and terror financing controls (measures) accordingly
- Systems and controls to accommodate:
  - Higher risk- enhanced controls required
  - Lower risk- lighter controls required.



# Risk-based approach

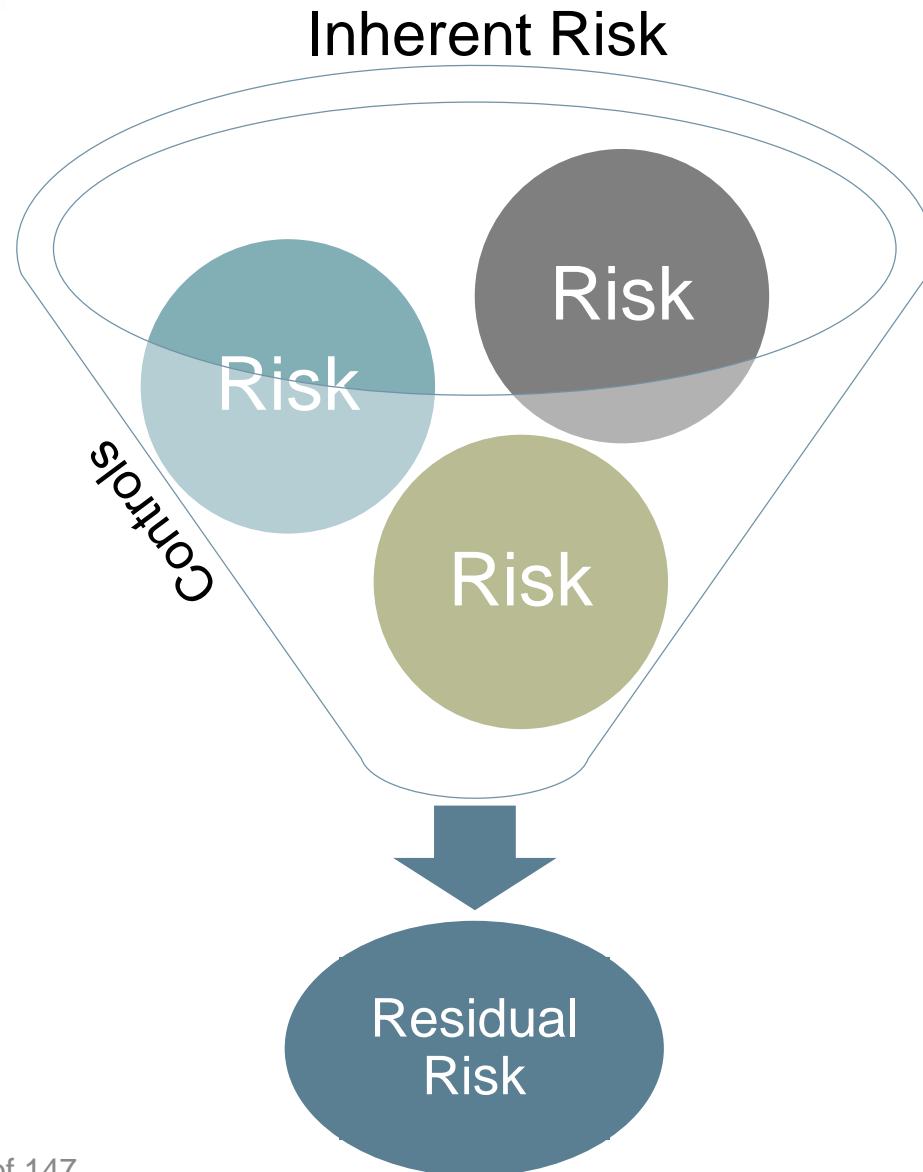


- **Methods to manage risk**

## **Mechanisms to manage risk**

- Systems, policies and procedures
- Awareness training
- Reporting
- Client and transaction analytics
- Process to exit high risk relationships
- Approval for high risk transactions and relationships
- Screening tools

# Risk-based approach



## Risk mitigation - treatment of risk

- Treatment of risk = systems and controls developed to manage the identified money laundering and terror financing risks i.e. clients and products
- Risk will be adequately treated = level of **residual risk** is acceptable & within the risk appetite of the accountable institution

## Practical treatment:

- Apply RBA when carrying out customer due diligence measures in respect identified money laundering and terror financing risks
- Higher money laundering/terror financing risk – more stringent due diligence
- Lower money laundering/terror financing risk – “lighter touch”

# Risk management and compliance programme

## WHO

- All Accountable Institutions
- Approved by, and responsible party are the board of directors

## WHAT

- Policy, procedures, systems and controls for money laundering risk-based approach

## WHEN

- Current, and ongoing reviews

## WHERE

- All subsidiaries within the AI space
- International application as the minimum standard

## WHY

- To understand money laundering and terror financing risk facing the entity, and to allocate the appropriate time and resources

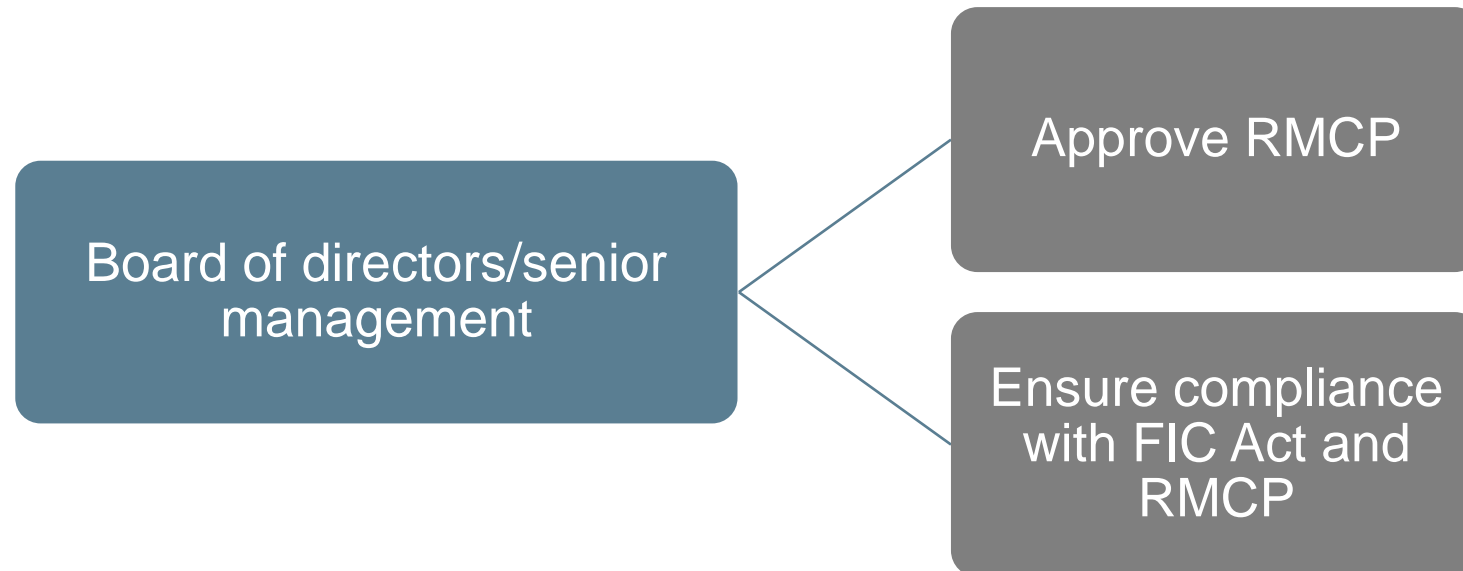
# Risk management and compliance programme

- Als must **develop**, **document**, **maintain** and **implement** a risk management and compliance programme (RMCP)
- RMCP is the foundation of the AI's efforts to comply with its FIC Act obligations
- RMCP must incorporate all the elements relating to
  - Policy
  - Procedure
  - Systems
  - Controls



# Risk management and compliance programme

- The effective implementation and application of a risk-based approach is largely dependent on the accountable institution's RMCP
- International operations – South African obligations are the minimum
- Review and update to the RMCP at regular intervals



# Risk management and compliance programme

## Unpacking the RMCP

Risk identification

Customer Due Diligence

Transactional monitoring

Record keeping

Reporting to the FIC

Extended registration model of entity

Implementation of RMCP

# Risk management and compliance programme

## Risk identification

- The risks that the products or services may involve or facilitate money laundering must be:
  - Identified
  - Accessed
  - Monitored
  - Mitigated
  - Managed

# Risk management and compliance programme

## Customer Due Diligence

- Identification if prospective client, or client who has established a relationship / once-off transaction
- Provisions relating to not dealing with anonymous and fictitious clients – section 20A
- Establishment and verification of client identification (CDD / KYC / FIC Act) – section 21
- Additional due diligence for legal persons, trusts and partnerships
- Ongoing due diligence
- Process when there are doubts about information or documentation received (veracity)
- Process to exit a relationship when customer due diligence cannot be conducted

# Risk management and compliance programme

## Customer due diligence

- How to determine if a client is a foreign prominent public official or domestic prominent influential person (politically exposed person or politically influential person)
- Process for enhanced due diligence for high risk clients
- Evidence how customer due diligence is linked to risk (low risk application vs high risk application)

# Risk management and compliance programme

## Transactional monitoring

- Manner in which future transactions will be consistent with knowledge of client
- Examination and records of
  - Complex/unusually large transactions
  - Unusual patterns that have no apparent business or lawful process

# Risk management and compliance programme

## Record keeping

- Customer due diligence and transactional information obtained – how and where will these records be kept?
  - Who will have access to these records
  - Measures in place to safeguard the records
  - 3<sup>rd</sup> party storage?
  - Electronic vs manual record keeping
  - How long will the records be kept (i.e. 5 years)

# Risk management and compliance programme

## Reporting to the FIC

- When is a transaction or activity reportable to the FIC
  - Suspicious or unusual transactions (STR)
  - Cash Threshold (CTR)
  - Terrorist Property and Target Financial Sanctions (TPR)
  - International Fund Transfer (IFTR)
- Timing of reporting (to tie in with provisions of FIC Act)
- Manner of reporting (i.e.. goAML, user access etc.)



# Risk management and compliance programme

## Extended registration model of entity

- When an entity has branches, subsidiaries or other operations in foreign countries
- Does the host country of the foreign branch permits FIC Act obligations or measures
- Advise the FIC accordingly
- South African requirements remain the minimum requirement (i.e. if in another country and if they have a lower standard than South Africa)

# Risk management and compliance programme

## Implementation of RMCP

- Process for implementing the risk management and compliance programme
  - Role definition in terms of application
  - Clear approval by senior management/board
  - Process to review and update risk management and compliance programme
  - Training on risk management and compliance programme.



THANK YOU

# Questions and discussion





# Contact Us

[www.fic.gov.za](http://www.fic.gov.za)

Compliance Contact Centre

012 641 6000