FIC ROADSHOW
Compliance obligations in
terms of the FIC Act
AGENDA

Compliance with the FIC Act

Registration and Reporting

Enforcement of the FIC Act
Status of the Financial Intelligence Centre Amendment Act

- The FIC Amendment Act, 2017 (Act No. 1 of 2017) was assented to on 26 April 2017
- On 13 June 2017 the Minister of Finance determined different dates for different sections of the Act to come into operation
  - 13 June 2017; and
  - 2 October 2017; and
  - First quarter 2018
- Consultation process with stakeholders on the draft regulations, withdrawal of exemptions as well as draft guidance to assist institutions to implement the FIC Amendment Act has been finalised
- All relevant documentation is available on our website www.fic.gov.za
Sections of the Amendment Act that came into operation on 13 June

• Some sections of the Amendment Act are not dependent on any subordinate legislation and came into operation on 13 June, such as-
  ➢ Repeal of provisions relating to CMLAC
  ➢ Inspections
  ➢ Appeals
  ➢ Sharing of information
  ➢ Arrangements for consultations with stakeholders

• These sections also do not impact directly on accountable institutions in terms of complying with their AML/CFT obligations
Steps to be taken before 2 October

• Certain sections of the Amendment Act require changes to current regulations and exemptions, such as-
  ➢ Customer due diligence measures
  ➢ Record keeping requirements
  ➢ Risk Management and Compliance Programme
  ➢ Governance and training

• The regulations must be finalised before or at the same time the sections come into operation

• Changes to regulations and exemptions require that Guidance be in place to assist institutions in meeting their obligations

• Require the publication of the draft Regulations and the Minister’s intention to withdraw Exemptions together with draft Guidance to be published for public comments (completed)
Documents published during consultation process

- Included in the published documents is a new approach by government to combat money laundering and terrorist financing
- Consultation sessions were held with industry bodies in the consultation process
- Notices in respect of amendments to Regulations and Exemptions will be submitted to the Minister for tabling in Parliament before the Minister publishes these in the Gazette
Changes to Regulations and Exemptions

- The draft regulations contain the following changes:
  - Prescribing a value for a transaction to be considered a “single transaction” – set at R5 000
  - Removing the detailed requirements on identification and verification requirements and compiling a client profile
  - Reporting regulations in line with reporting forms
  - Draft criteria for supervisory bodies (other than the SARB and FSB) to be able to request information from an accountable institution relating to STRs submitted to the FIC
  - Provide administrative sanctions for non-compliance with Regulations
- All exemptions will be withdrawn
Guidance to assist in the implementation of the new requirements

- Initial guidance will be generic, but must be adequate to assist accountable institutions with initial implementation of new requirements:
  - General principles in relation to implementing a risk based approach
  - Information on indicators to be taken into consideration when undertaking a risk assessment as well as understanding risk
  - Customer Due Diligence measures – including beneficial ownership and prominent persons
  - Obligations in respect of recordkeeping
  - The content of the Risk Management and Compliance Programme
  - The implementation of the targeted financial sanctions provisions
Supervision and enforcement – roles of SB and AI

**Supervisory Bodies**
- Engage with AIs regarding implementation, compliance and enforcement of FIC Act and new provisions
- Set clear milestones and timeframes for achieving compliance
- Priority based, incremental approach
- Monitor and guide AIs
- Inspections and other oversight activities during transition period

**Accountable Institutions**
- Demonstrate progress towards full compliance of FIC Act
- Adhere to milestones
- Engage with the Supervisory Body
Supervision and enforcement

- Sanctioning non-compliance with the new requirements of the FIC Act will be delayed in order to allow sufficient time for accountable institutions to make the necessary adjustments to implement.

- Enforcement of the provisions of the FIC Act that are not amended e.g. registration and reporting obligations will continue.

- At no point should accountable institutions not know who they are doing business with and must ensure that proper records are kept of transactional activities at all times.
Applicable sources of AML information

- **FIC Act**
  - Amended by FIC Amendment Act 1 of 2017

- **Money Laundering Control Regulations**
  - Withdrawn and amended
  - Substantial changes to CDD and internal rules
  - Changes to reporting

- **Guidance and Directives**
  - Guidance Notes/PCCs to be reviewed by the FIC
  - "old" guidance applicable to old regime

- **Exemptions**
  - Withdrawn

**IMPORTANT:**

The FIC Act, 2001 (Act 38 of 2001) still applies and there is no suspension, no vacuum, until 2 October 2017 when most sections of Amendment Act will become operational.
FIC Amendment Act Framework & New Compliance Concepts

- Risk Based Approach
- Targeted Financial Sanctions
- Risk Management and Compliance Programme
- Record Keeping
- Customer Due Diligence Measures
- Natural Persons
  - Legal Persons - Beneficial Ownership
  - Foreign Prominent Public Officials
  - Domestic Prominent Influential Persons
- Foreign Prominent Public Officials
- Domestic Prominent Influential Persons
FIC Amendment Act Framework & New Compliance Scene – 7 pillars of compliance

OLD

- Client Identification and verification
- Record keeping
- Reporting
- Formulate & implement internal rules
- Person responsible for Compliance
- Training of employees
- Registration with the FIC

NEW

- Client identification and verification
- Record keeping
- Reporting
- Risk Management Compliance Programme
- Person responsible for Compliance
- Training of employees
- Registration with the FIC

Risk based approach applied to CDD

Risk based approach applied
Risk Based Approach

• Previously rules bases system
• Which risks are we talking about?
• Risk = Money Laundering (ML) and Terrorist Financing (TF) risk

<table>
<thead>
<tr>
<th>Money Laundering</th>
<th>Terrorist Financing</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Proceeds of crime</td>
<td></td>
</tr>
<tr>
<td>• Placement, layering, integration</td>
<td></td>
</tr>
<tr>
<td>• Proceeds no longer associated with underlying criminal activity</td>
<td></td>
</tr>
<tr>
<td>• Proceeds appear legitimate</td>
<td></td>
</tr>
<tr>
<td>• Solicitation, collection and providing funds and assets with intention to be used to support terrorist acts, terrorist organisations and individual terrorists</td>
<td></td>
</tr>
<tr>
<td>• Illegal and legal sources</td>
<td></td>
</tr>
<tr>
<td>• Goal – to conceal financing and nature of activity being financed</td>
<td></td>
</tr>
</tbody>
</table>
Risk Based Approach

**Risk = Money Laundering (ML) and Terrorist Financing (TF) risk**

- Threats and vulnerabilities put accountable institution at risk of being abused to facilitate ML/TF activities
- Potential clients may use products and services offered by the accountable institution for ML/TF purposes
- Applying a RBA ensures that accountable institutions are able to ensure that measures to prevent ML/TF are in proportion with the ML/TF risks identified
Risk Based Approach

General principles of RBA

- Identify, assess and understand ML/TF risks posed
- Take measures to manage and mitigate the ML/TF risks
- Management & mitigation of risk means “treating” the risk
- Treatment of risk = systems and controls developed to manage the identified ML/TF risks
- Management of risk by developing control measures to mitigate risks identified
- Must be in proportion with extent of assessed risks
- Risk management mechanisms to take into account:
  - Consequence and impact of ML/TF risk
  - Likelihood of ML/TF risk occurring
Risk Based Approach

Risk Assessment

- Identify the ML/TF risk
- Take into account factors/indicators when assessing ML/TF risk
  - Products and services
  - Delivery channels
  - Geographic locations
  - Clients
  - Other factors
Risk Based Approach

Risk Rating

• Assign different categories to different levels of risk
• Will vary between different accountable institutions – no “one size fits all” approach
• Risk scale tailored to size of accountable institution and range of products offered
• Risk rating may change, re-evaluation of risk rating is critical
• Risk rating methodology must be documented in RMCP
Risk Based Approach

Risk mitigation - treatment of risk

- Treatment of risk = systems and controls developed to manage the identified ML/TF 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:

- Customer due diligence = measure to mitigate ML/TF risk
- Apply RBA when carrying out customer due diligence measures in respect identified ML/TF risks
- Higher ML/TF risk – more stringent due diligence
- Lower ML/TF risk – “lighter touch”
Risk Based Approach

ML/TF risk management

• Management of ML/TF risks = continuous cycle

• ML/TF risk management systems and controls must remain adequate – things change

• For example: monitor client behavior in relation to these risks – it may change

• Residual risk should also be reassessed at regular intervals
Customer Due Diligence Measures

- Risk Based Approach
- FIC Amendment Act
- Record Keeping

- Customer Due Diligence Measures
- Natural Persons
- Legal Persons - Beneficial Ownership
- Foreign Prominent Public Officials
- Domestic Prominent Influential Persons

- Risk Management and Compliance Programme
Customer Due Diligence Measures

Customer due diligence

- CDD process assists accountable institution to:
  - know who they are doing business with
  - know who benefits from the business it does with the client
  - understand the nature of the business it does with a client
  - determine when a transaction during that business relationship is considered suspicious or unusual

- Identification and verification of clients currently regulated by regulations and exemptions

- CDD expands client identification and verification

- RBA allows for more flexibility to exercise judgement in determining the extent and nature of the information required for CDD

- The findings of the risk assessment will determine the level and type of CDD that will be applied
Anonymous clients and single transaction threshold

No anonymous clients

- Accountable institutions may not do business with an anonymous client or client with apparent false or fictitious name

Single transaction threshold

- Value of the transaction to be determined by the Minister
- No requirement to carry out full CDD
- Should obtain and record some information about the client
Establishing the identity of the client

- CDD begins with an accountable institution knowing the identity of its client
- Establishing the client’s identity requires obtaining a range of information about the client
- Obtained from the client during the take on stage or part of the client engagement process
- Verification of the client’s identity is the corroboration of the information by comparing it against the original source or reliable third party
- Flexibility to choose the type of information to establish the client’s identity and the means to verify information obtained
- The nature and extent of the verification to be determined on the assessed risk and in terms of RMCP
- Verification must occur during the course of conducting the single transaction/business relationship but must complete the verification before it concludes a transaction
Establishing the identity of clients - natural persons

<table>
<thead>
<tr>
<th>Identification</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic level</strong></td>
<td>• Verification methods may vary</td>
</tr>
<tr>
<td>• Full names</td>
<td>• Verification with information obtained from</td>
</tr>
<tr>
<td>• Date of birth</td>
<td>a reliable and independent third-party</td>
</tr>
<tr>
<td>• Identifying number issued by government</td>
<td>source</td>
</tr>
<tr>
<td><strong>Supplementary information</strong></td>
<td>• As far as possible the original source of</td>
</tr>
<tr>
<td>• Biometric information</td>
<td>the information</td>
</tr>
<tr>
<td>• Place of employment or business</td>
<td></td>
</tr>
<tr>
<td>• Residential address</td>
<td></td>
</tr>
<tr>
<td>• Contact particulars</td>
<td></td>
</tr>
<tr>
<td>• Tax number</td>
<td></td>
</tr>
</tbody>
</table>
Establishing the identity of clients - natural persons

Examples of government issued or controlled sources of information:

- South African identity documents including smart card identity documents
- Valid driver’s license
- Foreign identity documents
- Passports
- Asylum seeker or refugee permits
- Work permits
- Visitor’s visas
Understanding the business relationship

- Accountable institutions are required to obtain additional information at the CDD stage of the business relationship including:
  - purpose and intended nature of the business relationship
  - source of funds to be used in business relationship
- The information should be sufficient to understand the client and the business relationship
Ongoing Due Diligence

- Scrutiny of transactions undertaken throughout the business relationship
- 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 ML/TF risks associated with business relationship with client
- Ongoing due diligence processes detailed in RMCP
Doubts about veracity of previously obtained information

- Accountable institutions are required to take certain measures
  - if there are doubts about the veracity of previously obtained CDD information
  - suspicion of ML or TF is formed at a later stage

- RMCP must set out the manner and process to
  confirm the CDD information when it has doubts about
  veracity of previously obtained information
Inability to conduct due diligence

- Prohibits accountable institution from entering into or maintaining business relationship or concluding single transaction if it cannot perform CDD
- If circumstances that prevents CDD are suspicious or unusual – consider report in terms of section 29
- RMCP 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 CDD
- RMCP should also provide for the manner in which it will terminate an existing business relationship when unable to complete CDD requirements
Foreign and domestic prominent persons

- Accountable institution must know who their clients are and understand their client’s business.
- Business with foreign prominent public officials must always be considered high risk.
- Business with domestic prominent influential persons are not inherently high risk.
- Being a prominent person **does not** create a presumption of being guilty of any crime and **does not** mean that an accountable institution cannot transact with such a person.
- Accountable institutions will have to include the management of business relations with person in prominent positions in their RMCP.
Domestic prominent persons

Domestic prominent influential persons includes:

- The President, Ministers and Premiers
- Members of the royal family and senior traditional leaders
- DGs and CFOs of government departments
- Executive mayors and municipal managers
- CEOs and CFOs of state entities like Eskom, Telkom, FIC, FSB, NGB, EAAB, etc.
- Judges
- Senior officials of companies that receive certain tenders from government

Includes family members and known close associates
Foreign prominent persons

Foreign prominent public officials includes:

- Head of State
- Members of a foreign royal family
- Government ministers
- Senior judicial officers
- Senior executives of state owned companies
- High ranking member of the military

Includes family members and known close associates
Foreign and domestic prominent persons

Where relationship with domestic prominent person poses a high risk OR dealing with a foreign prominent public official:

• Accountable institutions must do the following:
  ✓ Obtain senior management approval
  ✓ Establish source of wealth and source of funds
  ✓ Monitor the business relationship

• Monitoring the relationship means that close attention is paid to the manner in which the client uses the institutions services and products
Corporate vehicles identification and verification - additional due diligence measures applied

Corporate vehicles
- Legal persons
- Trusts
- Partnerships

Nature of client’s business

Ownership and control structure

Beneficial ownership
Legal persons, partnerships and trusts

In addition to verifying the identities of the clients which are not natural persons – accountable institutions need to:

- Understand the nature of its business
- Understand its ownership and control structure
- Know who the natural persons are who ultimately own or control their clients
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 accountable 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

<table>
<thead>
<tr>
<th>Characteristics which describes identity of legal person</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Name and trading name</td>
<td>- Accountable institution to decide on degree and methods of verification based on ML/TF risk</td>
</tr>
<tr>
<td>- Form</td>
<td>- methods may vary</td>
</tr>
<tr>
<td>- Registration number</td>
<td>- verification with information obtained from a reliable and independent third-party source</td>
</tr>
<tr>
<td>- Address of registered office/business address if different</td>
<td>- As far as possible the original source of the information</td>
</tr>
<tr>
<td>- Powers</td>
<td></td>
</tr>
<tr>
<td>- directors</td>
<td></td>
</tr>
<tr>
<td>- Senior management</td>
<td></td>
</tr>
<tr>
<td>- Tax numbers</td>
<td></td>
</tr>
</tbody>
</table>
Beneficial Ownership

Beneficial ownership requirements

- Institutions are required to establish who the beneficial owner of the legal person is and take reasonable steps to verify the beneficial owner’s identity.

Beneficial ownership?

- Beneficial ownership refers to the natural person(s) who owns or exercises effective controls the client

Application

- Beneficial ownership applies to legal persons, partnerships and trusts.
Beneficial Ownership

Legal persons, partnerships and trusts = vulnerable to be used for money laundering

The lack of adequate, accurate and timely beneficial ownership information facilitates ML/TF by disguising

✓ The identity of known or suspected criminals
✓ The true purpose of an account or property held by the legal entity
✓ The source or use of funds or property associated with the legal entity

The establishment of beneficial ownership is important for two reasons:

✓ Understand the customer profile to properly assess the ML/TF risks associated with the business relationship
✓ Take appropriate steps to mitigate the risks
Beneficial Ownership

Ownership & control structure – who is the beneficial owner?

Verification of BO

- methods may vary
- verification with information obtained from a reliable and independent third-party source
- As far as possible the original source of the information
- Process detailed in RMCP
Beneficial Owner Elimination Process – legal person

**Step 1: Who is the main shareholder/voter**
- The percentage of shareholding with voting rights = good indicator
- Ownership of 25% or more of shares/voting rights = good indicator

**Step 2: Who is natural person who exercises control through other means**
- e.g. through voting rights attaching to classes of shares or through shareholder

**Step 3: If no natural person can be identified**
- AI must determine who = natural person who exercises control over the management of the legal person
Partnerships

**Identification**
- Name – how partnership is known
- Partners

**Verification**
- Reasonable steps
- Based on ML/TF risk
- Partnership agreement
- Verification measures documented in RMCP

**Executive control - partnership**
- Section 21B(3)
- Identity of such a person
- Identity of each natural person authorized to enter into single transaction or business relationship on behalf of partnership

**Verification**
- Reasonable steps to verify
- Based on ML/TF risk
- Verification measures documented in RMCP
Trusts

**Identification**
- Name – unique name or description
- Registered with Master of High Court – unique reference number and address where trust registered

**Beneficial Owner – Trust**
- Section 21B(4)
- Identity of founder
- Identity of trustee and each natural person authorized to enter into single transaction or business relationship on behalf of trust
- Identity of named beneficiaries
- Particulars of how beneficiaries are determined

**Verification**
- Reasonable steps to verify
- Based on ML/TF risk
- Trust deed
- Verification measures documented in RMCP
Obligation to keep records

- Recordkeeping requirements will require accountable institutions to record adequate information to enable the reconstruction of the flow of funds to assist investigators in the event of a criminal investigation.

- Records may be kept in electronic form.

- The Centre, supervisory bodies and law enforcement must be able to readily access electronically stored records.

- Record keeping not dependent on risk levels and is fully applicable to customer due diligence.

- Record keeping procedures detailed in RMCP.
Obligation to keep records

- Keeping of customer due diligence records
- Record of all information obtained to comply with section 21 to 21H
- Keep record of all single transactions and transactions in course of business relationship
- Enable reconstruction of transaction:
  ✓ Amount
  ✓ Currency
  ✓ Date of transaction
  ✓ Business correspondence
  ✓ Identifying particulars of accounts and account files where applicable
Obligation to keep records

- 5 years from date the business relationship is terminated
- Records kept in terms of section 22A – 5 years from date on which the transaction is concluded
- Transaction or activity which gave rise to a section 29 report – 5 years from date on which report was submitted to the FIC
- Ongoing investigations – keep records until law enforcement agency has confirmed case has been closed
Risk Management and Compliance Programme

- Accountable institution must develop, document, maintain and implement a Risk Management and Compliance Programme (RMCP)
- RMCP must incorporate all the elements in the Act that are linked to the CDD measures
- The effective implementation and application of a risk-based approach is largely dependent on the accountable institution’s RMCP
Content of RMCP:

- How AI identifies, assesses, monitors, mitigates and manages ML/TF risk
- How AI determines if person is prospective/existing client
- How AI ensures “no anonymous clients”
- How AI identifies and verifies different types of clients and why
- How AI determines if future transactions consistent with AI’s knowledge of prospective client
- How AI conducts additional due diligence for legal persons, partnerships and trusts
- How AI conducts ongoing due diligence and account monitoring
- How AI examines and keep written findings of complex/unusually large transactions and unusual patterns of transactions/which have no apparent business/lawful purpose

“how” = manner in which & processes
Content of RMCP - continues:

- How AI will confirm information relating client where there are doubts about veracity of previously obtained information
- How AI will perform CDD in course of business relationship where AI suspects the activity/transaction is suspicious
- How AI will terminate existing business relationship if unable to conduct CDD
- How AI determines if prospective client is foreign/domestic prominent person
- How AI conducts enhanced due diligence for high risk relationships and when simplified CDD may be permitted
- How and where records are kept
Content of RMCP - continues:

- Enables AI to determine if transaction/activity is reportable to the FIC
- Provides process for reporting information to the FIC
- How the RMCP is implemented in branches, subsidiaries and other operations in foreign countries
- How the AI will determine if the host country or foreign branch/subsidiary permits implementation of measures required under the FIC Act
- How the AI implements its RMCP
Reporting

Suspectious Transaction Report (STR)
- Section 29
  - Suspicious and Unusual Transaction Report (STR)
  - Suspicious and Unusual Activity Report (SAR)
  - Suspicious and Unusual Transaction Report Batch (STRB)
  - Terrorist Financing Activity Report (TFAR)
  - Terrorist Financing Transaction Report (TFTR)

Cash Threshold Report (CTR)
- Section 28
  - Cash Threshold Report (CTR)
  - Cash Threshold Report Aggregation (CTRA)

Terrorist Property Report (TPR)
- Section 28A
  - Terrorist Property Report (TPR)
  - UNSC List

International Fund Transfer (IFTR)
- Section 31
  - International Fund Transfer (IFTR)
Cash Threshold Reporting – Current and FIC Amendment Act

• In terms of section 28 of the FIC Act

• Cash Threshold amount – R24 999,99

• Reportable 2 days from becoming aware of transaction

• Once off single transaction (CTR)

• Multiple related transactions (CTRA)
  ✓ 1 Business day (24 hours)
  ✓ Multiple business days

• Multiple reporting – cash received and cash paid (i.e. No set off)
Suspicious Transaction Reporting – Current and FIC Amendment Act

- In terms of section 29 of the FIC Act
- What is suspicious?
- Who must report?
  - a person who carries on a business
  - a person who is in charge of a business
  - a person who manages a business or
  - a person who is employed by a business

- NO cash threshold applicable
- When must reporting occur? No later than 15 working days from being aware
- Can one proceed with a transaction after reporting? Yes, section 33 of the FIC Act applicable
- Protection for person reporting? Yes, section 38 of the FIC Act applicable
Terrorist Property Reporting

- In terms of section 28A of the FIC Act
- Property owned or controlled by or on behalf of, or at the direction of:
  - Any entity which has committed or facilitated the commission of a specified offence as defined in POCDATARA
  - A specific entity identified in a notice issued by the President, under section 25 POCDATARA - This list is known currently as UN1267
- The knowledge about the origin and ownership of the property in question should be based on fact and should be acquired with reference to an objective set of circumstances or facts

FIC Amendment Act:

- Ceasing of business and reporting of person identified by Resolutions of United Nations Security Council (UNSC Resolution list)
- Notice will be given by the Director
Governance of AML/CFT compliance

Section 42A

- Board of directors/senior management are responsible for compliance with FIC Act and RMCP
- If AI is a legal person
  - compliance function assist the board of directors/senior management to comply with FIC Act and RMCP
  - Assign person (compliance officer) to ensure effectiveness of the compliance function - must be competent with sufficient seniority
- If AI is not a legal person
  - Person/s exercising highest level of authority must ensure compliance with FIC Act and RMCP
  - Appoint a person to assist such a person to comply with FIC Act and RMCP
Training of employees

• Training in terms of the FIC Act
• Training to be ongoing
• Enable employees to comply with the FIC Act and the RMCP
Registration with the FIC – current and Amendment Act

- New registration and reporting platform implemented in April 2016
- All Accountable and Reporting Institutions must register – section 43B
- Registration is done via the www.fic.gov.za website

New registrations
- Register as per user guides
- Entity AND user created in registration process
- ORG ID will then be generated
- Multiple registrations required per Item type
Implementation of UNSC resolutions

Administration of targeted financial sanctions by the FIC

• FATF Recommendation 7

• Member countries must implement TFS to combat financing of the proliferation (increase) of weapons of mass destruction and beyond

• TFS measures restrict sanctioned persons and entities from access to and financial services in relation to funds and property

• Accountable institutions must freeze property and transactions in accordance to financial sanctions imposed in the UNSC resolutions
Implementation of UNSC resolutions

Process – implementation

UNSC resolution

FIC publishes permission notices of MOF on website

Adoption notice published in GG by MOF

FIC Director publication of sanctioned individuals/entities on website

Process – maintenance of regime

UNSC resolution - update to lists

FIC send notification to stakeholders

Notification sent to FIC

FIC updates lists on FIC website
Implementation of UNSC resolutions

Role of the accountable institution - general

• Check if sanctioned person/entity is a client or prospective client

• May alert person/entity of status as sanctioned person/entity

• May not acquire, collect or use property of such persons/entity – prohibited

• May not transact or process transactions for sanctioned persons/entity

• Status quo as at time of imposition of sanction in relation to property or funds must be maintained and no financial services may be provided to the person or entity – except in instance where Minister of Finance has permitted certain financial services or dealings with the property

• Accountable institution must report to FIC the property in its possession/under control which is owned or controlled by or on behalf of a person or an entity identified on the sanctions list (section 28A)
Implementation of UNSC resolutions

Role of the accountable institution - screening

- Accountable institution must be able to identify sanctioned individuals
- Screening of existing clients and prospective clients against sanctions list
- When?
  ✓ Client take on process
  ✓ When new lists are adopted and published
Implementation of UNSC resolutions

Role of the FIC

- Maintain updated sanctions list available on website - sanctions lists will reflect available information on entities and persons contained in the notices published by the Director of the FIC
- Publish on FIC website notices of Minister’s permission to accountable institutions and others relating to
  - access to basic living expenses and the relevant conditions thereto
  - Provision of financial services or the dealing in affected property not related to basic living expenses, necessary in normal course of business e.g. accrual of interest or contractual payments
Amendments to Schedules

• Widening of scope of the FIC Act

• Include new business sectors in Schedule 1 of the FIC Act

• Additional categories of institutions and businesses as accountable institutions will improve the Centre’s ability to obtain information concerning the identities and financial activities of clients of a wider range of financial and other institutions

• This in turn will improve the Centre’s ability to provide high quality information to law enforcement and security agencies
Amendments to Schedules

- Increase in transparency of the financial system – whereby institutions gather information regarding client identity and nature of transactions that can be recorded and accessed over time.

- Will also bring South Africa’s legal framework against ML/TF in line with the international standards set by the FATF.

- South Africa was found to be deficient by not having certain categories of businesses included under the scope of the FIC Act.
Amendment of Schedules

Who should be considered to be included?

- As required by the FATF standards the following should be included under the scope of the FIC Act but are not yet included:
  - Professional accountants (consultation commenced)
  - Professionals providing services relating to the formation and administration of trusts and companies (TCSPs) (consultation commenced)
  - Dealers in precious metals and precious stones
  - Persons who carry on the business of a credit provider (consultation commenced)
  - Motor Vehicle dealers (consultation commenced)
Amendment of Schedules

Other industries under consideration:

- Numismatic dealers (looking to widen it to include coin dealers instead of limiting it to Kruger Rand dealers)
- Dealers in high value goods (need to identify who are dealers in high value goods; could be those that deal in precious metals and stones; yachts; etc.)
- Persons who carry on the business of providing private security boxes or security vaults for the safekeeping of valuables
- Short-term insurance industry (consultation commenced)
- Auctioneers (including a Sheriffs’ offices when performing the job of an auctioneer at a public auction)
- Persons who carry on the business of a virtual currency exchange eg. where Bitcoins may be bought or sold for SA currency (consultation commenced)
Contact Us

- www.fic.gov.za
- Compliance Contact Centre 012 641 6000
Registration and Reporting
Feedback
AGENDA

• goAML registration process overview
• goAML feedback and recommendations
  ✓ Common reporting errors
  ✓ When to report a Person, Entity or Account
  ✓ Feedback and recommendations
• Impact of the RBA on regulatory reporting
• Q&A
Registration

Steps to register on goAML if you have an ORG ID...

- You have an ORG ID if you previously had an AI or RI number.
- Phone the FIC Compliance Contact Centre on 012 641 6000 if you do not know your ORG ID.

You MUST register a person AND update your entity’s information.

Steps to register a person:
1. Have a scanned, clear copy of your ID and authorization letter available before starting.
2. Go to www.fic.gov.za and click on the button “Click here to Register or Report”.
3. Click on “Register” rather than “Register As Organisation”.
4. DO NOT select the “individual User” check box.
5. Insert your Org ID in the “Organisation ID” field.
6. Complete the rest of the requested information in full.
7. Remember to attach the Authorisation letter and ID.
8. Submit.
9. Wait for your approval confirmation email.

Steps to update your entity’s information:
1. Login with your username and password.
2. Click on “My GoAML” then “My ORG Details”.
3. Update all the fields with the latest information and contact details.
4. Submit.
5. Wait for your approval confirmation email.

Steps to register on goAML if you do not have an ORG ID...

- If you were never registered with the FIC.
- Phone the FIC Compliance Contact Centre on 012 641 6000 to confirm that you do not have an ORG ID.

Steps to register a new entity:
1. Have a scanned, clear copy of your ID and authorization letter available before starting.
2. Go to www.fic.gov.za and click on the button “Click here to Register or Report”.
3. Click on “Register” then “Register As Organisation”.
4. Complete all the requested information in full.
5. Remember to attach the Authorisation letter and ID.
6. Submit.
7. Wait for your approval confirmation email.

Select a good Password:
The password must be between 5 and 10 characters long and must include:
- One or more capital letters; AND
- One or more lower case letters; AND
- One or more numbers; AND
- One or more special characters (for example ! or @).
- An example is: goAML123@
goAML Common Reporting Errors

CTR and CTRA

• Transactional reports are reported with both sides of the transaction marked as “not my client”

• All transactions are “bi-party” transactions; with a “From”/sender and “To”/receiver side, and one of the sides has to be “my client”

• Incorrect cash threshold transactions aggregation - multiple transactions conducted by the same client (i.e. single client view) within the specified aggregation period should be reported as CTRA (considering the directionality of funds)

• Mandatory information sets are omitted, e.g. Swift Code, client ID/Passport Number and transaction mode/fund type (for CTR/CTRA FIC advises the use of “Cash received by AI/RI” or “Cash paid by AI/RI”)
goAML Common Reporting Errors

SAR and STR

- Mandatory information sets are omitted, e.g. “Reason/Reason for Reporting”, “Action”, client information (ID/Passport Number, Address, Telephone Number etc.)

- STR’s have been reported where a series of transactions are summarised

- Reporting Entities need to provide detailed descriptions / narratives in both the “Reason/Reason for Reporting” and “Action” fields

- NB - these free text fields should not be used to insert data that ought to be captured in other fields on the SAR/STR forms
goAML Common Reporting Errors

General

• Incorrect scenarios are reported
• Transactions may not be summarised but should be listed separately on the reporting form
• Free text fields should not be used to insert information that should be captured as structured data on the reporting form (i.e. client names, ID Numbers, address information, transactions etc.)
• Attachments are used to list information that ought to be captured on the goAML reporting form
• Reporting Entities default to “Unknown” for client and transaction information fields that they should have e.g. Address, Telephone Number, Account Type etc.
• Reporting Entities need to complete the reporting form in full with all information readily available and avoid only completing mandatory fields to enable the report to be processed on the FIC system
• Reports should be remediated as per the documented process (see goAML Web Notice 04)
The relationship between person, entity and account when reporting a transaction on the reporting platform of the FIC (goAML).

<table>
<thead>
<tr>
<th>FROM</th>
<th>TO</th>
<th>Person</th>
<th>Entity</th>
<th>Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person</td>
<td>e.g. Person 1 pays Person 2</td>
<td>e.g. Person pays Entity</td>
<td>e.g. Person makes a cash deposit into personal account at Bank</td>
<td></td>
</tr>
<tr>
<td>e.g. Person pays Person 2</td>
<td>cash for goods/services in person</td>
<td>cash for goods/services on premises</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entity</td>
<td>e.g. Entity pays Person cash</td>
<td>e.g. Entity pays Entity</td>
<td>e.g. Entry A makes cash deposit into business account at Bank</td>
<td></td>
</tr>
<tr>
<td>refund for goods/services</td>
<td>Entity</td>
<td>cash for goods/services on premises</td>
<td></td>
<td></td>
</tr>
<tr>
<td>on premises</td>
<td>on premises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td>e.g. Person makes a cash</td>
<td>e.g. Conductor from Entity A makes a cash</td>
<td>e.g. Electronic payment between two accounts</td>
<td></td>
</tr>
<tr>
<td>makes a cash</td>
<td>withdrawal at Bank ATM</td>
<td>withdrawal in Bank branch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Person makes a cash</td>
<td>Account</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>withdrawal at Bank ATM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e.g. Person makes a cash</td>
<td>withdrawal in Bank branch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>withdrawal at Bank ATM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e.g. Person makes a cash</td>
<td>withdrawal in Bank branch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>withdrawal at Bank ATM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Regulatory Reporting – Recommendation for Reporting Entities

1. **Reporting Entities need to maintain their registration/user information:**
   - Directive 1 instructs Reporting Entities to maintain their details on the FIC platform
   - Directive 2 instructs that users are not allowed to share user credentials

2. **Reporting Entities need to ensure they apply the latest version of the goAML schema:**
   - goAML no cost implications (i.e. subscription charges or licensing fees)
   - Entities that elect to automate their regulatory reporting submissions will be provided with free software (B2B) to assist with the automation process
   - Reporting Entities remain responsible for any in-house development or customisation of regulatory reporting services (see B2B documents)
   - Updates to the FIC schema (**current version is 4.2.2**), lookup lists and business rules are communicated in advance - timeously test and roll-out the updates
3. **Reporting Entities need to provide frequent and practical training to their employees:**

- Reporting Entities should ensure that their staff receive adequate training.
- Staff training should include practical sessions that enable staff to successfully submit regulatory reports on goAML (i.e. utilising the FIC UAT site).
- FIC published a registration user guide, regulatory reporting user guides, guidance (e.g. Guidance Note 05B and goAML Notices) and scenario examples to assist external entities to train their staff.
- These publications must be used together with the Regulations to ensure that users are trained effectively and that Reporting Entities discharge their obligations accordingly.
4. **Reporting Entities need to supply the FIC with all readily available information:**

- FIC continuously encounters instances were Reporting Entities are omitting information that is readily available

- Reporting Entities need to complete the reporting form in full with all information readily available and avoid only completing mandatory fields to enable the report to be processed on the FIC system

- Reporting Entities should ensure that their reporters are trained properly and have access to all relevant source systems to successfully submit regulatory reports with the FIC
5. **Reporting Entities need to conduct on-going reviews of submitted regulatory reports:**

- Reporting Entities should conduct regular reviews of all regulatory reports submitted to ensure it meets the prescribed requirements.

- The FIC has noted that many entities have drafted web reports that remain **unresolved**; not-submitted web reports as well as rejected reports that have not been fixed and resubmitted.

- This indicates a deficiency in the internal controls (e.g. monitoring) that a Reporting Entity needs to apply to ensure regulatory reports are submitted within the prescribed time period and format.

- The FIC has already contacted Reporting Entities in this regard, and the matter will subsequently be escalated to the applicable Supervisory Bodies.

- Reporting Entities should therefore conduct frequent sampling as the reporting responsibility should not be deferred to the ICT Department or developers - multi-disciplinary approach.
6. Reporting Entities need to review their internal reporting processes and verify that all the products and services offered are mapped and reported correctly:

• Reporting Entities should have documented reporting process that outlines the steps to be followed for the detection, monitoring, reporting and remediation of regulatory reports submitted to the FIC

• The processes should outline the steps to be followed internally to conduct pre-validation and remediation of source systems

• Reporting processes should be applied consistently across all business areas and should incorporate the regulatory reporting timeframes specified (i.e. 48 hours for CTR/CTRA and 15 days for SAR/STR etc.)
goAML Web Reporting Tips

- Failed/rejected regulatory reports must be remediated as per the defined process (see goAML Web Notice 04)

- Web reports that have been rejected must be reverted back to draft status, edited and re-submitted

- The FIC noted in excess of 2400 rejected regulatory reports to date remain in draft status; either the Reporting Entity has captured a new report, or has not yet remediated the rejected report. In both scenarios the Reporting Entity is considered to be non-compliant!

- We advise all users to clear/delete their browsing histories frequently and restart their browsers afterwards - deletion of cookies and passwords

- The FIC does not accept any regulatory reports submitted unless it was submitted on the goAML system
goAML Web Reporting Tips

• Always ensure that web reports are saved before submitting it on goAML Web

• Available attachments (e.g. copy of ID/Passport, contract or deposit slip) may be uploaded and submitted with the initial report submitted to the FIC

• To upload attachments with a web report - save the report and thereafter add multiple attachments

• Download copies of all submitted regulatory reports (web and batch) along with the report receipts and save on the AI’s internal systems for record keeping purposes

• Frequently download copies of all submitted regulatory reports and report receipts - archived after 30 days. The FIC will not provide copies to any parties

• When pulling statistics on goAML Web limit the date range searches to be no longer than 30 days

• Entities that submit large volumes of reports must download the statistical reports on a daily basis as the maximum amount of rows to be returned is 10 000

• Always report any goAML incidents/queries to the FIC immediately by means of the formal channels
The RBA will have a limited impact on the FIC’s regulatory reporting requirements:

- AI’s would still need to identify their clients and report this information to the FIC.
- The FIC regulatory reporting forms will allow for the selection and/or insertion of “Not Obtained” in certain client information fields to allow for instances where the information would not be obtained.
- As part of their RMCP, AI’s would have to apply enhanced due diligence to products and services deemed to be susceptible to ML and TF.
- AI’s need to report information that is readily available to enable a transaction to be commercially viable.
- The RBA should not be used selectively to report minimal information sets to the FIC, but rather all readily available information which the AI would have obtained in the course of its regular business.
Registry and Compliance Glossary

AI/RI refers to an Accountable Institution (listed in Schedule 1 to the FIC Act) and Reporting Institution (listed in Schedule 3 to the FIC Act).

CO
Compliance Officer refers to a person who is tasked, for purposes of the registration and reporting process, to ensure that the details of the accountable institutions are correctly submitted and maintained on the FIC’s website, and regulatory reports are submitted successfully.

MLRO
Money laundering reporting officer is envisaged to be a person, other than the CO, with the responsibility and authority to submit regulatory reports to the Centre on behalf of the AI/RI. Not all AI/RI will have MLROs. MLRO will have his/her own login credentials on goAML. goAML will have his/her own login credentials on goAML.

goAML
refers to the an integrated software solution implemented by the Centre as its preferred IT platform for registration, reporting, data collection, analysis, case management and secure communications required for the Centre’s daily operational functions and requirements.

ORG ID
An Org ID will be assigned to the AI/RI in goAML, and will be used by an institution as the unique identifier for that institution. It allows goAML users belonging to that particular institution to have access to information relating to that institution.

TPR
refers to a terrorist property report submitted to the Centre in terms of section 28A of the FIC Act.

CTR
Cash Threshold Report contains unrelated cash transactions whereby each transaction on its own has exceeded the threshold (R24 999.99) and no aggregation is demonstrated.

Cash
Cash is defined in section 1 of the FIC Act as: coin and paper money of SA or another country; and travellers’ cheques. EFT is not considered cash.

CTR A
Cash Threshold Report Aggregation is a cash threshold report of aggregates of smaller amounts which when combined add up to the prescribed amount, in cases where it appears to the AI/RI concerned that the transactions involving those smaller amounts are linked in such a way that they should be considered fractions of one transaction.

STR
means a Suspicious and Unusual Transaction Report which must be submitted in terms of section 29(1) of the Act in respect of the proceeds of unlawful activities or money laundering where the report relates to a transaction or series of transactions between two or more parties.

SAR
means a Suspicious and Unusual Activity Report which must be submitted in terms of section 29(1) of the Act in respect of the proceeds of unlawful activities or money laundering where the report relates to an activity which does not involve a transaction between two or more parties.

TFTR
means a Terrorist Financing Transaction Report which must be submitted in terms of section 29(1) of the Act in respect of the financing of terrorism and related activities where the report relates to a transaction or series of transactions between two or more parties.

TFAR
means a Terrorist Financing Activity Report which must be submitted in terms of section 29(1) of the Act in respect of the financing of terrorism and related activities where the report relates to an activity which does not involve a transaction between two or more parties.

FOR MORE INFORMATION VISIT WWW.FIC.GOV.ZA OR CONTACT THE COMPLIANCE CONTACT CENTRE ON 012- 641 6000 (SELECT OPTION 1)
Contact Us

- www.fic.gov.za
- Compliance Contact Centre 012 641 6000
Enforcement of the FIC Act
AGENDA

• Supervision of the FIC Act
• Enforcement of the FIC Act
• Appeals
FIC Act Supervision & Enforcement Model

• Supervisory Bodies (SBs) take responsibility to supervise and enforce compliance with the FIC Act, order, determination or directive made in terms of the FIC Act by all accountable institutions (AIs) regulated or supervised by it [s45(1)]

• The FIC takes responsibility to supervise and enforce non-compliance with the FIC Act on AIs and RIs not regulated or supervised by a SB [s4(g)(i)]

• The FIC takes responsibility to supervise and enforce non-compliance with the FIC Act on AIs regulated or supervised by a SB where the SB fails to fulfil its responsibilities [s4(g)(ii), 45(3), 45B(6)(a)]
Inspections in terms of the FIC Act

- The purpose of inspections in terms of the FIC Act is to determine the level of compliance of the AI [s45B(1)]

- The FIC and SBs cannot use the inspections powers to investigate any criminal conduct

- Should the FIC or SB detect any criminal conduct during an inspection, it may refer the matter to law enforcement to investigate

- The allegations of criminal conduct may be an indication that an AI has not complied with the FIC Act and may lead to an inspection
Inspections in terms of the FIC Act

• Inspectors must be in possession of the certificate when conducting inspections [s45A(5)]

• An inspector must show his certificate when requested by an effected person or person in charge of the premises [s45A(5)]

• Inspection done at reasonable time and within ordinary business hours [s45B(1D)]

• Inspection done on reasonable notice where appropriate [s45B(1D)]

• Inspectors require a warrant to conduct inspections on unlicensed businesses or a private residence unless consent is given by the person apparently in control of the business and/or the occupant of the private residence [s45B(1A)-(1C)]
Inspections in terms of the FIC Act

Inspections are to be done with strict regard to an affected person’s right to:

✓ Dignity
✓ Freedom and security
✓ Privacy and
✓ Other constitutional rights and

With strict regard to decency and good order as the circumstances require in particular:

✓ Entering and inspecting only such areas or objects as are reasonably required
✓ Conducting inspections discreetly and with due decorum
✓ Causing as little disturbance as possible and
✓ Concluding the inspection as soon as possible
# Scope of inspections

The sections in **red** come into effect on 2 October 2017

The sections in **yellow** may be withdrawn/amended

<table>
<thead>
<tr>
<th>Duty</th>
<th>Section</th>
<th>Applicable Regulations</th>
<th>Applicable directives, guidance notes or PCCs</th>
<th>Applicable exemptions</th>
<th>Administrative sanction</th>
<th>Criminal sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer due diligence (Identify and verify client)</td>
<td>20A, 21, 21A, 21B, 21C, 21D, 21E, 21F, 21G, 21H</td>
<td>3 to 19 &amp; 21</td>
<td>GN 1, 2, 3 PCC03, 03A, 08, 09, 10, 11, 14, 15, 20, 21, 22, 24, 26, 27, 29, 30, 31, 32, 33</td>
<td>2 to 16</td>
<td>R50 million for legal person R10 million for natural person</td>
<td>N/A</td>
</tr>
<tr>
<td>Duty to keep records</td>
<td>22, 22A 23 &amp; 24</td>
<td>20 &amp; 26</td>
<td>PCC02</td>
<td>3 to 17</td>
<td>R50 million for legal person R10 million for natural person</td>
<td>N/A</td>
</tr>
<tr>
<td>Reporting duties</td>
<td>28; 28A &amp; 29</td>
<td>22; 22A; 22B; 22C; 23; 24; 27A; 27B &amp; 27C</td>
<td>Dir 3, GN 4 &amp; 5 PCC04, 16, 28, 36, 37</td>
<td>N/A</td>
<td>R50 million for legal person R10 million for natural person except STR</td>
<td>R100 million or 15 years imprisonment</td>
</tr>
<tr>
<td>Risk Management and compliance programme (Formulating and implementing of internal rules)</td>
<td>42</td>
<td>25; 26 &amp; 27</td>
<td>PCC 19, 35</td>
<td>N/A</td>
<td>R50 million for legal person R10 million for natural person</td>
<td>N/A</td>
</tr>
<tr>
<td>Training relating to AML &amp; CFT</td>
<td>43</td>
<td>N/A</td>
<td>PCC 18</td>
<td>N/A</td>
<td>R50 million for legal person R10 million for natural person</td>
<td>N/A</td>
</tr>
<tr>
<td>Governance of AML &amp; CFT (appointment of the compliance officer)</td>
<td>42A</td>
<td>N/A</td>
<td>PCC 12</td>
<td>N/A</td>
<td>R50 million for legal person R10 million for natural person</td>
<td>N/A</td>
</tr>
<tr>
<td>Registration with the Centre</td>
<td>43B</td>
<td>27A</td>
<td>Dir 1, 2, 4, GN05 PCC05, 06, 07, 13, 17, 23, 25, 34</td>
<td>N/A</td>
<td>R50 million for legal person R10 million for natural person</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Inspections conducted
Inspection findings

FIC Inspections

- Compliant: 116
- Non-compliant: 16
Failed to identify and verify clients
Failed to register on time
Failed to monitor for terrorist property reports
Failed to register and report reportable transactions
Failed to report cash threshold transactions
Failed to report cash threshold & suspicious transactions
Inspection findings

Reasons advanced for non-compliance

- Lack of diligence: 57
- Ignorance: 17
- Lack of data: 6
- Employee at fault: 4
- No access to reporting system: 4
- Other: 6

Financial Intelligence Centre
Common inspection findings

1. Registration:
   - Branches of institutions are not registered
   - Institutions did not register a user on goAML

2. Identification & verification of clients:
   - Legal entities are not identified and verified as prescribed in Regulations 7, 8, 15 & 16
   - Misinterpretation and/or application of the exemptions to the FIC Act
   - Dispute on when and what constitutes a business relationship
   - AIs receive money from clients without identifying and verifying the client first
3. **Cash threshold reporting**
   - Cash received in the bank account of the AI is not reported by the AI (confusion on dual reporting)
   - Some cash threshold transactions are not reported where the institution employs centralised reporting
   - CTRs are not reported timeously

4. **Terrorist property reporting**
   - No or inadequate screening of clients
Common inspection findings

5. Suspicious & unusual transaction reporting
   • Neither the compliance officer nor the employees knows what a suspicious transaction is in their environment
   • The training provided to the employees of the institution is not adequate or frequent enough
   • No ‘defensive’ reporting when receiving a subpoena or section 27 request

6. Internal rules
   • The internal rules are not customised for the particular business
   • Internal rules are not implemented or adhered to by the AI or its staff
   • Accountability and responsibilities are not specified in the internal rules
Common inspection findings

7. Appointment of the compliance officer
   - No replacement of a compliance officer that resigned
   - Sharing of login credentials to file reports

8. Training
   - No one remembers the training
   - The FIC Act is not readily available
Supervision of a risk based approach

- It is expected that very few institutions will be compliant with the amendments to the FIC Act by 2 October 2017.
- Enforcement of the amendments to the FIC Act will be delayed by the FIC and supervisory bodies in order to give time to accountable institutions to implement the amendments to the FIC Act.
- Enforcement of the provisions of the FIC that are not amended will continue e.g. registration and reporting obligations.
- The FIC and supervisory bodies will work together in deciding when to start enforcing the amendments to the FIC Act. The decision to enforce will be informed by the readiness survey.
- Accountable Institutions will not be able to use the risk based approach to remediate non-compliance failures identified during previous inspections. Remediation of non-compliance identified during inspections needs to continue.
Supervision of a risk based approach

• Inspections by the FIC and supervisory bodies will continue as usual. The inspections will be used to monitor, guide and advise accountable institutions on implementation of the risk based approach.

• Accountable institutions must use the provisions of the current Act until they are ready to comply with the amendments to the Act.

• Supervisors will not conduct an independent risk assessment, but will not necessarily accept a risk assessment as correct.

• Focus on high-level issues, not fine details and should take a common-sense approach to whether the results are reasonable.
Supervision of a risk based approach

Technical assessment

- Does the RMCP comply with the Act & guidance?
- Test the rigour of the processes and procedures used and internal consistency of the assessment
- Consider other credible or reliable sources of information to identify whether there might be any material differences that should be explored further

Effectiveness assessment

- Does the AI adhere to their own RMCP?
- Inspect client files
- Interview employees

Governance assessment

- Role of the Board, executive or senior management & compliance function
- Sign off, reviewing and updating of RMCP
## Sanctions issued 2016/2017

<table>
<thead>
<tr>
<th>Institution</th>
<th>Contravention</th>
<th>Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eddies Motors</td>
<td>Failure to file CTRs</td>
<td><strong>R21 787.50</strong>&lt;br&gt;50% suspended for two years and a directive to remediate</td>
</tr>
<tr>
<td>Travcor t/a York Motors</td>
<td>Failure to file CTRs</td>
<td><strong>R76 091</strong>&lt;br&gt;50% suspended for two years and a directive to remediate</td>
</tr>
<tr>
<td>D &amp; L Motors</td>
<td>Failure to file CTRs</td>
<td><strong>R35 294.25</strong>&lt;br&gt;Entire amount suspended for two years and a directive to remediate</td>
</tr>
<tr>
<td>Squad Cars</td>
<td>Failure to file CTRs</td>
<td><strong>R201 400</strong>&lt;br&gt;50% suspended for two years and a directive to remediate</td>
</tr>
<tr>
<td>Mr Kruger- Magalieskruin</td>
<td>Failure to file CTRs</td>
<td><strong>R78 268</strong>&lt;br&gt;R50 000 payable – remainder suspended for two years and a directive to remediate</td>
</tr>
<tr>
<td>Noordrand Motors</td>
<td>Failure to file CTRs</td>
<td><strong>R106 870</strong>&lt;br&gt;50% suspended for two years and a directive to remediate</td>
</tr>
</tbody>
</table>
## Sanctions issued 2016/2017

<table>
<thead>
<tr>
<th>Institution</th>
<th>Contravention</th>
<th>Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tangawizi Motors</td>
<td>Failure to file CTRs</td>
<td><strong>R225 646</strong> 50% suspended for two years</td>
</tr>
<tr>
<td>Habib Overseas Bank Limited</td>
<td>Failure to implement internal rules</td>
<td><strong>R1 million</strong></td>
</tr>
<tr>
<td></td>
<td>Failure to file STRs</td>
<td></td>
</tr>
<tr>
<td>Investec Bank Limited</td>
<td>Failure to identify and verify clients</td>
<td><strong>R20 million</strong> and directive to remediate</td>
</tr>
<tr>
<td></td>
<td>Failure to implement internal rules</td>
<td></td>
</tr>
<tr>
<td>South African Bank of Athens Limited</td>
<td>Failure to identify and verify clients</td>
<td><strong>R3 million</strong>, reprimand and directive to remediate</td>
</tr>
<tr>
<td></td>
<td>Failure to implement internal rules</td>
<td></td>
</tr>
<tr>
<td>Standard Chartered Bank</td>
<td>Failure to identify and verify clients</td>
<td><strong>R10 million</strong>, a reprimand and directive to remediate</td>
</tr>
<tr>
<td></td>
<td>Failure to file CTRs</td>
<td></td>
</tr>
</tbody>
</table>
## Sanctions issued 2016/2017

<table>
<thead>
<tr>
<th>Institution</th>
<th>Contravention</th>
<th>Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Société Generale Johannesburg Branch</td>
<td>Failure to identify and verify clients</td>
<td><strong>R2 million</strong> penalty conditionally suspended for two years and directive to remediate</td>
</tr>
<tr>
<td></td>
<td>Failure to keep record</td>
<td></td>
</tr>
<tr>
<td>ABSA</td>
<td>Failure to identify and verify clients</td>
<td><strong>R10 million</strong> and directive to remediate</td>
</tr>
<tr>
<td>Imali Express (Pty) Ltd</td>
<td>Failure to file TPR</td>
<td>Reprimand</td>
</tr>
<tr>
<td></td>
<td>Failure to appoint a person to ensure compliance</td>
<td><strong>R10 million</strong></td>
</tr>
<tr>
<td>Tourvest Financial Services (Pty) Ltd t/a American Express</td>
<td>Failure to register</td>
<td><strong>R150 000</strong>, with R50 000 conditionally suspended and directive to remediate</td>
</tr>
<tr>
<td>GBS Mutual Bank</td>
<td>Failure to identify and verify clients</td>
<td><strong>R500 000</strong>, reprimand and directive to take remedial action</td>
</tr>
<tr>
<td></td>
<td>Failure to implement internal rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failure to train staff</td>
<td></td>
</tr>
</tbody>
</table>
Administrative sanctions

• Previously any financial penalty imposed had to be paid into the Criminal Assets Recovery Account (CARA) established by s63 of POCA

• Now any financial penalty has to be paid into the National Revenue Fund s45C(7)(a)

• An administrative sanction imposed does not constitute a previous conviction in terms of the Criminal Procedure Act

• The administrative sanction has to be made public unless exceptional circumstances are present
Appeals

• An institution may appeal the decision of the Director or SB

• The appeal must be lodged within 30 days of receiving the sanction notice

• The appellant must, with the appeal, pay a fee of R10 000 to the FIC – regulation 27C (d)

• If the Appeal Board sets aside the decision of the FIC or SB, the R10 000 must be refunded to the appellant – s45D (10)(a)

• If the Appeal Board varies a decision of the FIC or SB, it may direct that the whole or part of the R10000 be refunded to the appellant – s45D (10)(b)

• Any party to an appeal is entitled to be represented at an appeal by a legal representative – s45D (6)
Appeals

- The Appeal Board has decided on two appeal matters i.e. JSH Motors t/a Honda Johannesburg South and Cotizone (Pty) Ltd t/a Cash Inn

- The following salient points can be extracted from the judgments:
  - Ignorance of the FIC Act is not an excuse and sanctions may be issued by the FIC or supervisory bodies despite the institution not knowing about their obligations, but it may lead to a reduced penalty
  - Financial penalties may be imposed on first time offenders
  - Wilful non-compliance should be met with harsh penalties
• Remediation of the non-compliance is a mitigating factor that should be taken into account when the appropriate sanction is considered

• The purpose of sanctioning is deterrence

• The Appeal Board referred with approval to the guidance issued by the FIC in order to resolve issues in dispute

• The FIC did not fail in its duty to supervise the institutions that do not have a supervisory body.
“The world suffers a lot. Not because of the violence of bad people, but because of the silence of good people”