




Financial
Intelligence Centre

A large, abstract geometric pattern on the left side of the page, composed of various shades of blue and grey triangles and polygons, creating a sense of depth and movement.

REFERENCE GUIDE FOR ALL ACCOUNTABLE INSTITUTIONS

Contents

1. INTRODUCTION.....	4
2. WHAT IS THE FINANCIAL INTELLIGENCE CENTRE?.....	4
3. WHAT IS MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING?	4
4. WHAT AMENDMENTS HAVE BEEN MADE TO THE SCHEDULES TO THE FIC ACT?.....	5
5. WHAT ARE THE OBLIGATIONS FOR ACCOUNTABLE INSTITUTIONS?.....	6
6. HOW DO ACCOUNTABLE INSTITUTIONS REGISTER WITH THE CENTRE?	6
7. WHAT IS A RISK-BASED APPROACH.....	8
8. WHAT IS A RISK MANAGEMENT AND COMPLIANCE PROGRAMME	8
9. WHAT IS CUSTOMER DUE DILIGENCE?	8
10. HOW DO ACCOUNTABLE INSTITUTIONS DETERMINE WHETHER CLIENTS ARE POLITICALLY EXPOSED PERSONS?.....	9
11. WHAT ARE TARGETED FINANCIAL SANCTIONS?.....	9
12. WHAT IS TRANSACTION MONITORING.....	10
13. WHAT REGULATORY REPORTS NEED TO BE SUBMITTED TO THE CENTRE....	10
14. WHAT ARE THE ASPECTS RELATED TO RECORD-KEEPING	11
15. WHAT TRAINING OF EMPLOYEES DO ACCOUNTABLE INSTITUTIONS NEED TO IMPLEMENT	11
16. WHAT IS THE COMPLIANCE FUNCTION FOR ACCOUNTABLE INSTITUTIONS?	12
17. CAN ACCOUNTABLE INSTITUTIONS OUTSOURCE THEIR OBLIGATIONS?	12
18. WHAT SOURCES OF INFORMATION CAN ACCOUNTABLE INSTITUTIONS USE?	12
Directives issued by the Centre.....	13
Guidance issued by the Centre	14
Risk assessments conducted by the Centre	21
Case studies	24
Scams awareness	24
Financial Action Task Force Guidance	24
19. COMMUNICATION WITH THE CENTRE	25
Table 1: Schedule item guidance	6
Table 2: Directives issued by the Centre	13
Table 3: Guidance Notes issued by the Centre	15

Table 4: Guidance Notes issued by the Centre21
Table 5: Sector risk assessments issued by the Centre22
Table 6: Summary of sections, regulations and associated guidance23

Figure 1: Compliance obligations in terms of the FIC Act.....6

1. INTRODUCTION

The Financial Intelligence Centre (the Centre) has issued this reference guide to assist all new, and existing accountable institutions. This guide provides an overview of who the Centre is, what the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (the FIC Act) requires from accountable institutions (in the form of FIC Act compliance obligations) and directs accountable institutions to the range of issued guidance material that is available. Accountable institutions are strongly encouraged to view all material through the links provided in this document as it provides valuable information that can aid in effective compliance with the FIC Act.

2. WHAT IS THE FINANCIAL INTELLIGENCE CENTRE?

The FIC Act was enacted in 2001, which directed the establishment of the Centre. The Centre was subsequently established in 2003 as the national centre for the gathering and analysis of financial data. The Centre's primary role is to contribute to safeguarding the integrity of South Africa's financial system and its institutions, and to make them intolerant to money laundering, terrorist financing and proliferation financing abuse, which directly underpins the integrity and stability of the financial sector. The Centre is the South Africa's financial intelligence unit.

3. WHAT IS MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING?

- **Money laundering** is the process that criminals use to launder their funds so that the proceeds they have acquired from illicit (illegal) activities appear to be legitimate.
- **Terrorist financing** is the process of funding terrorists, terrorist acts or terrorist organisations .
- **Proliferation financing** is where individuals, entities, countries or governments raise funds in order to assist with their purchasing of weapons of mass destruction.

The FIC Act lists institutions which are deemed to be vulnerable to being abused by criminals for money laundering, terrorist financing or proliferation financing purposes.

4. WHAT AMENDMENTS HAVE BEEN MADE TO THE SCHEDULES TO THE FIC ACT?

Schedule 1 to the FIC Act has been amended, whereby additional items, called accountable institutions, have been included to bring in new categories of businesses. Certain items have been amended to either widen current items or cater for technical amendments. All reporting institutions listed in Schedule 3 of the FIC Act have been deleted. The detailed list of Schedules amendments can be [found here](#).

Where appropriate, guidance has been published to provide further information on specific items. Listed below lists is guidance that has been issued regarding the amended items. All guidance is available on the FIC website, www.fic.gov.za.

Item	Description	Guidance explaining the definition & risk indicators
Item 1	Legal practitioners	Draft PCC 47A
Item 2	Trust and company service providers	Draft PCC 6A
Item 4	Authorised user of an exchange	
Item 7A	Co-operative banks	
Item 8	Life insurers	
Item 11	Credit providers	Draft PCC 23A
Item 12	Financial services providers	
Item 16	Ithala Development Finance Corporation* deleted (will now fall under item 11 of credit providers)	
Item 19	Money or value transfer provider	Draft PCC 118
Item 20	High-value goods dealers	Draft PCC 119
Item 21	South African Mint Company (RF) Pty Limited	

Item 22	Crypto asset service providers	Draft PCC 120
Item 23	Clearing system participants	

Table 1: Schedule item guidance

5. WHAT ARE THE OBLIGATIONS FOR ACCOUNTABLE INSTITUTIONS?

Accountable institutions are subject to certain obligations in terms of the FIC Act:

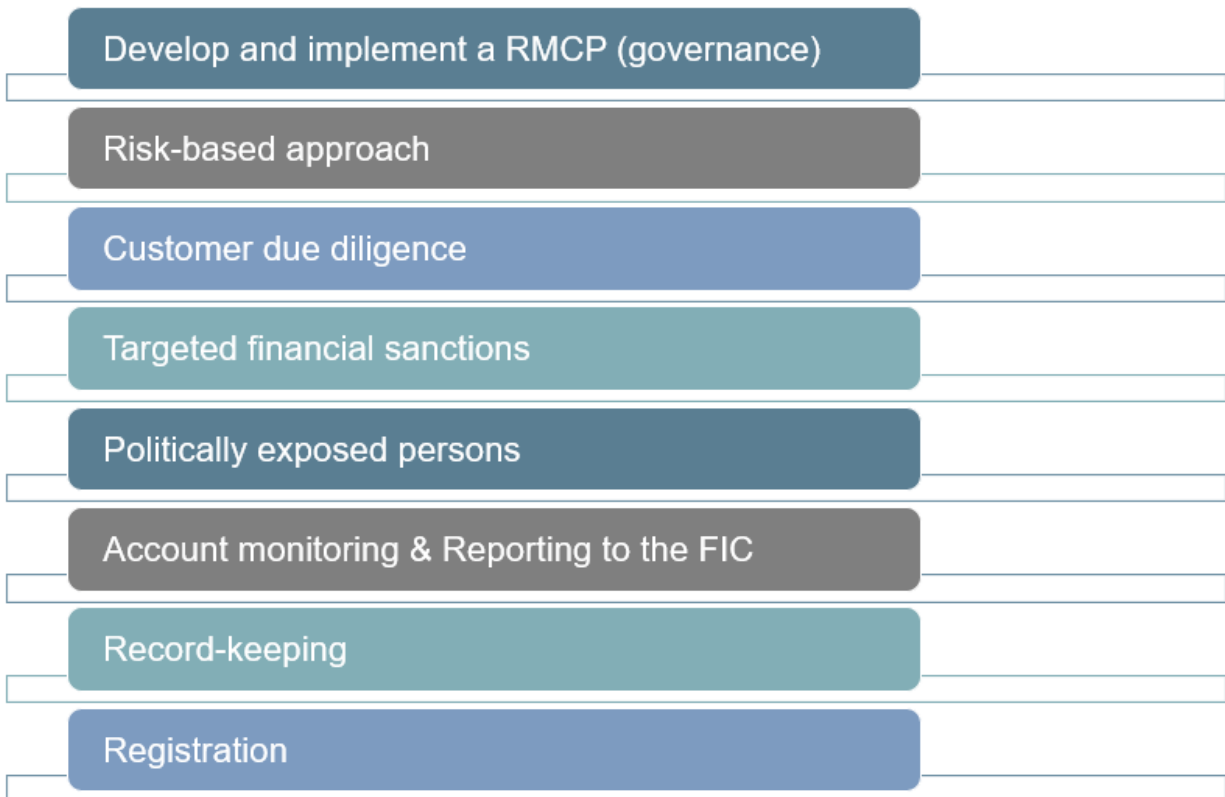


Figure 1: Compliance obligations of accountable institutions in terms of the FIC Act

6. HOW DO ACCOUNTABLE INSTITUTIONS REGISTER WITH THE CENTRE?

Before any accountable institution can submit a regulatory report to the Centre, they must register with the Centre via its reporting and registration system. Registration is free and must be completed via the Centre's online registration and reporting system called goAML, which is accessible via the website www.fic.gov.za. For further

guidance on how to register refer to the [goAML User Guide](#) and public compliance communication (PCC) 5D.

There are three simple steps to registering with the Financial Intelligence Centre:

- **Step 1 – Access the platform:** Go to the Centre’s website www.fic.gov.za, click on “click here to report or register” which will give the user access the goAML platform
 - **Step 2 – Register the entity:** Register the entity, and receive an ORG ID (organisation identity) number
 - **Step 3 – Register the compliance officer:** The accountable institution’s compliance officer must use the ORG ID number received to register as a user against the entity profile. The compliance officer **MUST** be the first person to register.
- This is practically done by:
 - **Capturing ALL information correctly and attaching the correct documents**
Complete all necessary fields on the goAML system (both for the organisation and user) and make sure to attach the following -
 - A certified copy of an identity document/passport of the compliance officer; and
 - A signed authorisation letter from the entity when registering
 - Must be on the letterhead of the entity; and
 - Must contain the username and surname; and
 - Identity or passport number, occupation of the user; and
 - The role of the user to be allocated on the system.
 - Bear in mind:
 - **Wait for the registration to first be approved by the Centre**
Once the registration form has been submitted electronically via the system, a registration reference number (SHREG number), will be provided. The reference number must be used for any registration related enquiries.
 - **Confirmation of registration will be sent after approval**

The compliance officer will receive an e-mail from the Centre confirming the approval or rejection of the registration and will confirm the entity's Org ID number.

7. WHAT IS A RISK-BASED APPROACH

Accountable institutions must implement a risk-based approach (RBA) to combating money laundering, terrorist financing and proliferation financing (ML, TF and PF.) An RBA entails implementing controls that are proportionate to the level of ML, TF and PF risk identified. Accountable institutions must conduct risk assessments on a business level, client level and on in regard to new products and processes.

Guidance Note 7 and public compliance communication (PCC) 53 sets out guidance on a risk-based approach.

8. WHAT IS A RISK MANAGEMENT AND COMPLIANCE PROGRAMME

Accountable institutions must develop, document, maintain and implement a risk management and compliance programme (RMCP.) An RMCP should be unique to the accountable institution. Section 42 of the FIC Act sets out what controls must be contained in the RMCP. The RMCP must be easily accessible upon request of the supervisory body or an employee of the accountable institution.

For further guidance on how to develop and document an RMCP refer to Guidance Note 7 and PCC 53.

9. WHAT IS CUSTOMER DUE DILIGENCE?

In order to combat ML, TF and PF all accountable institutions must identify and verify their clients. Customer due diligence (CDD) refers to the knowledge that an accountable institution has about its clients and the institution's understanding of the

business that the client is conducting with it. The level of identification and verification must be determined in line with the client's risk profile.

For further guidance on how to conduct CDD refer to [Guidance Note 7](#).

10. HOW DO ACCOUNTABLE INSTITUTIONS DETERMINE WHETHER CLIENTS ARE POLITICALLY EXPOSED PERSONS¹?

Accountable institutions are required to determine whether their client is a foreign prominent public official (FPPO) or domestic prominent influential person (DPIP.) Various methods may be used to determine these categories of persons, and often the client themselves is a source in this regard.

For further guidance on DPIPs and FPPOs, refer to [PCC 51](#).

11. WHAT ARE TARGETED FINANCIAL SANCTIONS?

Section 28A of the FIC Act requires all accountable institutions to scrutinise client information to identify designated persons or entities who are listed on the:

- Targeted financial sanction (TFS) list as published in terms of section 26A of the FIC Act, which is found on the FIC website, and
- TFS list as published in terms of section 25 of Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act 33 of 2004) (POCDATARA Act) which is found on the United Nations Security Council website.

This requirement is not risk-based and must be applied to all prospective clients regardless of risk. Accountable institutions must not provide products or services to designated persons or entities.

For further guidance on South Africa's TFS regime, refer to [PCC 44](#) and [PCC 54](#).

¹ Politically exposed persons or PEPs is a term used to describe foreign prominent public officials and domestic prominent influential persons

12. WHAT IS TRANSACTION MONITORING

Accountable institutions must scrutinise single transactions and transactions undertaken throughout the course of the business relationship with the client, to determine whether the transactions are aligned to the accountable institution's knowledge of the client and the client's business within the context of the clients ML, TF and PF risk profile. Transaction monitoring is aimed at identifying suspicious and unusual transactions and large cash payments.

For further guidance on transactional monitoring, refer to [Guidance Note 7](#), [Directive 5](#) and [PCC 45](#) which discusses the use of an automated transaction monitoring system.

13. WHAT REGULATORY REPORTS NEED TO BE SUBMITTED TO THE CENTRE

Accountable institutions must report to the Centre. There are three main regulatory reporting obligations for accountable institutions:

- **Cash threshold reports** (cash received or issued exceeding R49 999.99). The threshold has recently been increased by an amendment to the Regulations to the FIC Act.
- **Suspicious and unusual transaction reports** – where the reporter suspects that a transaction or activity involves money laundering, terrorist financing or a contravention of financial sanctions.
- **Terrorist property reports** – where an accountable institution has in its possession property of a designated person.

Accountable Institutions are required to submit regulatory reports electronically via the goAML system. If a regulatory report is rejected, it must be remediated by the accountable institution.

Refer to:

[Guidance Note 5C](#) and the [CTR reporting user guide](#).

Guidance Note 4B and the [STR reporting user guide](#)

Guidance Note 6A and the [TPR reporting user guide](#).

PCC 50 and the User Guide on Remediation of rejected Reports on how to remediate

14. WHAT ARE THE ASPECTS RELATED TO RECORD-KEEPING

Accountable institutions must keep records of client identification and verification information for a period of five years from the termination of the business relationship, transactional information for a period of 5 years from the date a transaction is concluded, and regulatory reports submitted to the Centre for the period 5 years from submitting a transaction or activity report contemplated in section 29 of the FIC Act. Refer to section 23 of the FIC Act. Records may be kept in electronic form.

Regardless of the manner in which records are kept, accountable institutions must ensure that the following principles are applied:

- The accountable institution must have free and easy access to the relevant records.
- The records must be readily available to the Centre and the relevant supervisory body when required.
- The records must be capable of being reproduced in a legible format and
- If the records are stored off-site, the Centre and the relevant supervisory body must be provided with the details of the third party storing the records.

15. WHAT TRAINING OF EMPLOYEES DO ACCOUNTABLE INSTITUTIONS NEED TO IMPLEMENT

The FIC Act does not specify the format of the required training, but it is the Centre's view that training provided by the accountable institution should enable its employees to comply with the provisions of the FIC Act and the accountable institution's RMCP.

16. WHAT IS THE COMPLIANCE FUNCTION FOR ACCOUNTABLE INSTITUTIONS?

The accountable institution must have a compliance function to assist the board of directors or the senior management of the accountable institution in discharging their obligations and assign a person with sufficient competence and seniority to ensure the effectiveness of the compliance function contemplated above.

Refer to [Draft Directive 6](#) and [Draft PCC 116](#) which details the obligation relating to employee screening.

17. CAN ACCOUNTABLE INSTITUTIONS OUTSOURCE THEIR OBLIGATIONS?

Accountable institutions remain responsible for their compliance obligations in terms of the FIC Act. They may, however, seek assistance in certain instances but cannot share passwords or information relating to suspicious and unusual transaction reports.

For further information on outsourcing of compliance obligation to third parties service providers refer to [PCC 12A](#)

18. WHAT SOURCES OF INFORMATION CAN ACCOUNTABLE INSTITUTIONS USE?

Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act)

The FIC Act is the prevailing legislation for anti-money laundering and counter terrorist financing in South Africa. All obligations that accountable institutions must adhere to, are contained in the FIC Act.

Money Laundering and Terrorist Financing Control Regulations

The Regulations should be read alongside the FIC Act, as they provide prescribed information that is not specified in the FIC Act.

Other legislation forming part of the anti-money laundering and counter terrorist financing or terrorism regime

The FIC Act works in conjunction with the Prevention of Organised Crime Act, 1998 (Act 121 of 1998) (POCA.) which criminalises the act of money laundering and other offenses.

ThePOCDATARA Act criminalises the offence of terrorist financing, and other offences involving terrorist acts and similar offences.

Directives issued by the Centre

The Centre has issued seven Directives:

Number	Topic	Link to access
Directive 1	Updating of registration information of accountable and reporting institutions	Link
Directive 2	Use of login credentials following registration with the Centre	Link
Directive 3	Notification of failure to report as required by the FIC Act	Link
Directive 4	Notification to Accountable Institutions registered prior to 7 March 2016 to update their registration details on goAML	Link
Directive 5	Prescribe the requirements for the usage of an automated transaction monitoring system (ATMS) for the detection and submission of regulatory reports to the Centre	Link
Draft Directive 6	Requires accountable institutions to screen employees	Link
Directive 7	The risk and compliance return	Link

Table 2: Directives issued by the Centre

Guidance issued by the Centre

The Centre issues guidance to the public on its statutory function in terms of section 4(c) of the FIC Act read together with Regulation 28 of the Money Laundering and Terrorist Financing Control Regulations issued in terms of the FIC Act. The different types of guidance include, but are not limited to:

- Guidance notes
- Public compliance communications (PCCs)
- User guides
- Webinars.

All guidance notes, PCCs, user guides and notices are available on the Centre's website.

Below are the active guidance products that can be consulted for further assistance. Also shown are guidance products that have been withdrawn and the products that have replaced them.

Guidance Note	Topic	Link to access
Guidance Note 1 (30 April 2004)	Guidance concerning identification of clients	Replaced by Guidance Note 7
Guidance Note 2 (18 June 2004)	Guidance to financial services industries regulated by the Financial Services Board concerning the meaning of the word “transaction”	Replaced by Guidance Note 7
Guidance Note 3 (GN 27803; 18 July 2005)	Guidance to banks on customer identification and verification and related matters	Replaced by Guidance Note 7
Guidance Note 4B (26 March 2019)	Guidance on suspicious transaction reporting	Link
Guidance Note 5C (21 October 2022)	Guidance on Cash Threshold Reporting	Link
Guidance Note 6A (27 March 2019)	Guidance on terrorist property reporting	Link
Guidance Note 7 (2 October 2017)	Implementation of the FIC Act	Link
Draft Guidance note 7A (30 September 2022)	Chapter 4: Updates to RMCP	In consultation, Link

Table 3 Guidance Notes issued by the Centre

The below table lists all PCCs issued by the Centre

Number	Topic	Link to access
PCC01	Establishment of the PCC series	Link
PCC02	Period for record-keeping of matters reported to the Centre	Replaced with Guidance Note 7
Revised PCC03A	Supplementary information applicable to PCC03 electronic verification systems of asylum seeker and refugee permits	Replaced with Guidance Note 7
PCC04	Obligations arising from the FIC Act pertaining to the voluntary disclosure programme	Withdrawn
PCC05C (9 May 2018)	Registration with the Centre by accountable and reporting institutions and acquisition of login credentials by any other business with a reporting obligation under the FIC Act	Link
PCC06	Clarity on Item 2 of Schedule 1 of the FIC Act	
Revised PCC07	The definition of a motor vehicle dealer for the purposes of Schedule 3 of the FIC Act	
PCC08	Duties of estate agents including provisions of exemption 11 in terms of the FIC Act	Replaced with Guidance Note 7
PCC09	Identification and verification of loyalty programme members in the casino industry in terms of the FIC Act.	Replaced with Guidance Note 7
PCC10	The client of an estate agent	Replaced with Guidance Note 7
PCC11	The closing of a client's account by an accountable institution amounts to a transaction in terms of the FIC Act.	Replaced with Guidance Note 7
PCC12	Outsourcing of compliance activities to third parties	Link

Number	Topic	Link to access
PCC12A	Outsourcing of compliance activities to third parties	
PCC13	Scope of item 12, Schedule 1 to the FIC Act.	Link
PCC14	Client identification and verification requirements when a person acts on the authority of another.	Replaced with Guidance Note 7
PCC15	The acceptance of a smart card document issued by the department of Home Affairs for client identification and verification purposes.	Replaced with Guidance Note 7
PCC16	Interpretation of the term “readily available information” for the purposes of cash threshold reporting in terms of the FIC Act.	Replaced with Guidance Note 5C
PCC17	Definition of Kruger rand dealer for purposes of the FIC Act.	Link , to be withdrawn
PCC18	Training and appointment of a compliance officer by accountable institutions in terms of Section 43 of the FIC Act.	Replaced with Guidance Note 7
PCC19	Formulation and implementation of internal rules for different accountable institutions within a complex group structure.	Replaced with Guidance Note 7
Revised PCC20	Client identification and verification requirements for non-face-to-face transactions online betting transactions.	Replaced with Guidance Note 7
PCC21	Scope and application of exemption 17 in terms of the FIC Act.	Replaced with Guidance Note 7
PCC22	Client identification and verification requirements in relation to international or foreign data protection laws	Replaced with PCC 22A
PCC23	The scope and meaning of Item 11 of Schedule 1 to the FIC Act.	Link
Revised PCC24	Verification requirements of South African companies and close corporations in terms of the FIC Act.	Replaced with Guidance Note 7

Number	Topic	Link to access
PCC25	Scope of Item 12 to the FIC Act	Link
PCC26	Single client view	Replaced with Guidance Note 7
PCC27	Status of expired documents relating to client identification and verification requirements for asylum seeker and refugees in terms of the FIC Act.	Replaced with Guidance Note 7
PCC28	Terrorist property reporting obligations for accountable institutions.	Replaced with Guidance Note 6A
PCC29	Clarity on the application and use of exemption 4	Replaced with Guidance Note 7
PCC30	Customer identification and verification of casino junket agents and their underlying clients in terms of the FIC Act.	Link
PCC31A	The acceptance of funds by an accountable institution prior to the completion of the prescribed client identification and verification requirements.	Link
PCC32	The scope of cross-border remittance exemption to the FIC Act	Replaced with Guidance Note 7
PCC33	Use of the Department of Home Affairs HANIS verification service for SABRIC member banks to establish and verify the identity of a client in terms of the FIC Act.	Replaced with Guidance Note 7
PCC34	Facilitation of reporting to the FIC for institutions from 8 March to 22 April 2016	Replaced with Guidance Notes 4C, 5B and 6A
PCC35	Failure of the control, processes and working methods of an accountable institution in relation to formulation and implementation of internal rules in terms of Section 42 of the FIC Act.	Replaced with Guidance Note 7

Number	Topic	Link to access
PCC36	Obligations arising from the FIC Act pertaining to the 2016 Special Voluntary Disclosure Programme	Link
PCC37	Obligations of reporting institutions in terms of the FIC Act.	Link
PCC 38A	The mode of communication regarding sections 27, 32, 34 and 35 of the FIC Act.	Link
PCC 39 (07 August 2018)	To mandated entities in relation to access by authorised officers to information held by the Financial Intelligence Centre	Link
PCC 40 (05 February 2019)	Licensing, registration, approval or authorisation conditions issued by supervisory bodies to accountable institutions,	Link
PCC 41 (20 December 2019)	Guidance on combating the financing of terrorism and anti-money laundering measures relating to non-profit organisations	Link
PCC 42 (28 February 2020)	Guidance on the disclosure of facts or information contained in section 29 reports, or providing a copy of such a report to a supervisory body in terms of section 29(3) and section 45(b)(2b) of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001)	Link
PCC 43 (27 February 2020)	Guidance on customer due diligence in relation to shared clients of accountable institutions	Link
PCC 44 (20 March 2020)	Guidance on the application of the targeted financial sanctions regime within South Africa	Link
PCC 45 (20 March 2020)	Guidance on Directive 5 of 2019 in relation to the use of automated transaction monitoring systems	Link

Number	Topic	Link to access
PCC 46 (30 March 2020)	Guidance on the commencement and enforcement of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) as amended by the Financial Intelligence Centre Amendment Act, 2017 (Act 1 of 2017)	Link
PCC 47 (25 March 2020)	Guidance on the interpretation of item 1 of Schedule 1 to the Financial Intelligence Centre Act, 2001 (Act 38 of 2001)	Link
PCC 48 (21 July 2020)	Guidance on certain life insurance business issues including customer due diligence and understanding of risk in relation to their client in terms of the FIC Act.	Link
PCC49 (29 March 2021)	Guidance on money laundering, terrorist financing risk and proliferation financing considerations relating to geographic areas	Link
PCC 50 (31 March 2021)	Guidance on the measures required for the mitigation of loss of intelligence data due to reporting failures	Link
PCC 51 (3 December 2022)	Guidance on measures relating to foreign prominent public officials and domestic prominent influential persons, their immediate family members and known close associates.	Link
PCC 52 (25 March 2022)	Guidance on the identification of money laundering and terrorist financing risks and associated customer due diligence for clients of authorised users of an exchange in terms of the FIC Act.	Link
PCC 53 (August 2022)	Guidance on the RMCP for DNFBPs	Link
PCC 54 (30 September 2022)	Guidance on the combatting of proliferation financing. Raising of risk awareness regarding proliferation financing.	Link

Number	Topic	Link to access
PCC 56 (14 November 2022)	Guidance to property practitioners on which persons are regarded as estate agents for purposes of the schedule 1 to the FIC Act.	Link
PCC 22A (30 November 2022)	Guidance on information processing in terms of the FIC Act in relation to the Protection of Personal Information Act 2013 (Act 4 of 2013)	Link

Table 4: Guidance Notes issued by the Centre

Risk assessments conducted by the Centre

An aspect of the risk-based approach is for the institutions to be able to identify and assess the ML/TF/PF risks they face. The first step in this process is to determine the risk at a national and sectoral level for the industry that the institution is situated in.

The Centre has identified the inherent ML risks and vulnerabilities facing seven sectors in South Africa, at a national level and a sectoral level. The national risk assessment is currently in process, while the several sector risk assessments are available on the Centre's website.

Risk title	Short description	Link to access
South African National Terrorism Financing Risk Assessment (12 April 2022)	The assessment identifies the terrorism financing risks and vulnerabilities currently facing South Africa.	Link
Gambling sector (31 March 2022)	This assessment identifies the inherent money laundering and terrorist financing risks currently facing the gambling sector in South Africa.	Link

Motor vehicle dealers' sector (31 March 2022)	This assessment identifies the inherent money laundering and terrorist financing risks currently facing the motor vehicle dealers' sector in South Africa.	Link
Lender of money against the security of securities sector (31 March 2022)	This assessment identifies the inherent money laundering and terrorist financing risks currently facing the lender of money against the security of securities sector in South Africa.	Link
Trust services providers' sector (31 March 2022)	This assessment identifies the inherent money laundering and terrorist financing risks currently facing the trust services providers' sector in South Africa.	Link
Real estate sector (17 March 2022)	This assessment identifies the inherent money laundering and terrorist financing risks currently facing the real estate sector in South Africa.	Link
Kruger rand dealers (17 March 2022)	This assessment identifies the inherent money laundering and terrorist financing risks currently facing the Kruger rand dealers sector in South Africa.	Link
Legal practitioners (17 March 2022)	This assessment identifies the inherent money laundering and terrorist financing risks currently facing the legal practitioners sector in South Africa.	Link

Table 5 Sector Risk Assessments issued by the Centre

Below is a summary of various sections in the FIC Act, and associated regulations and penalties for non-compliance.

Compliance duty		Section	Regulations	Directives, guidance notes and PCCs		Administrative sanction	Criminal sanction
Customer due diligence		20A, 21, 21A to 21H	N/A	GN 7		Natural person = R10 million Legal person = R50 million	N/A
Record-keeping		22, 22A, 23 & 24	20	GN 7		Natural person = R10 million Legal person = R50 million	N/A
Reporting	CTR	28	22, 22B & 22C, 24	Dir 3	GN 5C	Natural person = R10 million	15 years or R100 million
	TPR	28A	22, 22A, 23B, 23C, 24		GN 6A	Legal person = R50 million	
	STR	29	22, 23, 23A, 24	Dir 5	GN 4B	N/A	
Risk management and compliance programme		42	N/A	GN 7		Natural person = R10 million Legal person = R50 million	N/A
Training		43	N/A	GN 7		Natural person = R10 million Legal person = R50 million	N/A
Governance of AML and CFT		42A	N/A	GN 7		Natural person = R10 million Legal person = R50 million	N/A
Registration		43B	27A	Dir 2, PCC 5D		Natural person = R10 million Legal person = R50 million	N/A

Table 6 Summary of sections, regulations and associated guidance

Case studies

The Centre publishes on their website identified cases of criminals using different types of crimes to accumulate or gather their proceeds. The Centre publishes case studies and indicators to raise awareness on some of the methods criminals use. The page for this can be [accessed here](#).

Scams awareness

The Centre publishes samples of some of the notices and messages that scammers send to the public. If you think you may have been the subject of a scam, please access the scam awareness [page here](#).

The Centre also publishes scams awareness provided my money remitters. This page can be [accessed here](#).

Financial Action Task Force Guidance

The Financial Action Task Force (FATF) is an intergovernmental standard setting body for AML/CFT. The FATF standards include 40 Recommendations that all its member countries and members of FATF Style Regional Bodies (FSRBs) need to comply with. Members conduct peer reviews – that is, members assess other members' adherence to the Recommendations. South Africa was recently assessed, and the mutual evaluation report following this assessment was published in October 2021.

FATF also issues guidance to its member countries through its publications. FATF guidance is not directly binding on accountable institutions in South Africa, as the country needs to consider and apply their own economic characteristics. However, FATF guidance principles are highly informative and useful.

19. COMMUNICATION WITH THE CENTRE

The Centre has a dedicated compliance contact centre geared to assist accountable institutions to understand their registration obligations in terms of the FIC Act. Please call the compliance contact centre on 012 641 6000 and select option 1.

Compliance queries may also be submitted online by clicking on: <http://www.fic.gov.za/ContactUs/Pages/ComplianceQueries.aspx> or visiting the Centre's website and submitting an online compliance query.

To submit an online compliance query:

- Go to the Centre's website, www.fic.gov.za.
- Select "Contact the FIC" banner in the middle of the webpage.
- Select "Log a compliance query." using the drop-down list.
- Complete the information requested in as much detail as you can. The more detailed the query the easier it is for the Centre to provide a response.

Issued By:

The Director

Financial Intelligence Centre

15 December 2022