Office: 010 597 0835 | **Facilitator:** 083 821 8801 | **E-mail:** anna@compliancelearningcenter.net
Website: www.compliancelearningcenter.net |
Address: 10A Lever Street Brackenhurst Alberton, South Africa
Registration nr: 2018/242685/07 | **Vat nr:** 4070281904

Study Guide

AMENDED FINANCIAL INTELLIGENCE CENTRE ACT: ONLINE CPD COURSE 2020 / 2021

Anna Bouhail©

December 2019

Course summary

The amended Financial Intelligence Center Act course is a short course detailing the new requirements imposed on accountable and reportable institutions in terms of the Financial Intelligence Centre Amendment Act 1 of 2017.

The course has been updated in December 2019 to include ML/TF risk management concepts.

Time allotted for course

The course consists of 4 topics with an assessment that needs to be completed. The time allotted for each aspect is as follows:

Topic number	Title	Number of pages to read	Topic level	Time allotted
Topic 1	Introduction to FICA	7	Introductory	20 minutes
Topic 2	Main duties imposed on accountable institutions	21	Introductory	45 minutes
Topic 3	Measures to promote compliance by accountable institutions	4	Introductory	5 minutes
Topic 4	Administrative sanctions and penalties	2	Introductory	5 minutes
	Assessment			15 minutes
	Total time			**1.5 hours**

© Anna Bouhail

Assessment and certification

After completion of the workshop the learner must complete an electronic assessment on the learning management system.

- **Form of assessment:** Multiple Choice Questions
- **Number of questions**: 15 questions
- **Duration:** 60minutes
- **Competency mark:** 65%

Upon obtaining a competency mark of 70% the learning will receive a certificate of completion. The learner will be afforded an opportunity to re-do the workshop should a competency mark not be attained.

Course accreditation

CPD Category: Online programme

COB Category: All Classes of Business

Financial Planning Component: Ethics & Practice Standards

Advice Component: Ethics, Standards and Compliance

Accreditation valid until: 31 December 2020

CPD Points allocated: 1.5 hours | points

FPI approval number: FPI19120022

© Anna Bouhail

Table of contents

Copyright notice

© 2020 by Anna Bouhail

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

For permission request write to the author at the address below:

Anna Bouhail
10A Lever Street
Brackenhurst
Alberton
1449
South Africa

Ordering information
If you would like to order the publication, please contact author at address above.

TOPIC 1 INTRODUCTION TO FICA

LEARNING OUTCOMES

After studying the topic, the learner should be able to-

- Outline the purpose of the Financial Intelligence Centre Act
- Define concepts relating to the Financial Intelligence Centre Act

1.1 Abbreviations

The following is a list of abbreviations used in this text:

- **AI:** Accountable institutions
- **CDD:** Client due diligence
- **EDD:** Enhanced due diligence
- **FICA:** The Financial Intelligence Centre Act
- **FIC:** The Financial Intelligence Centre
- **FSP:** Financial Services Providers
- **KYC:** Know you client
- **MLRO:** Money Laundering Reporting Officer
- **ML/TF:** Money-laundering / Terrorist Financing
- **PEP:** Political exposed person
- **RMCP:** Risk Management and Compliance Program
- **STR:** Suspicious Transaction Report
- **TFS:** Targeted financial sanctions
- **UNSC:** United Nations Security Council

1.2 Introduction

The purpose of the Financial Intelligence Centre Act (FICA) is to combat money laundering activities and the financing of terrorist and related activities.

FICA pursue this objective by establishing the Financial Intelligence Centre (FIC). Furthermore, FICA bestows certain duties on accountable institutions to enable FIC to perform their statutory duties.

Money laundering is an activity that conceals the nature and source of proceeds that has been obtained illegally.

Terrorist financing refers to the processing of funds to sponsor or facilitate terrorist activity. Terrorist financing involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations.

In the case of money laundering, the funds are always of illicit origin, whereas in the case of terrorist financing, funds can stem from both legal and illicit sources. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the funding activity and the nature of the funded activity.

Similar methods are used for both money laundering and the financing of terrorism. In both cases, the actor makes an illegitimate use of the financial sector. The techniques used to launder money and to finance terrorist activities/terrorism are terribly similar and, in many instances, identical.

1.3 Definitions

A client may be regarded as anyone who uses the services of an accountable institution. Client categories include natural persons, companies, close corporations, trusts and partnerships.

A business relationship is an arrangement between a client and an accountable institution for concluding either a single transaction or transactions on a regular basis. Accountable institutions are listed in the Table following.

Table 1.1: Accountable institutions

An attorney	Foreign exchange dealer
A board of executors or a trust company or any person that invests, keeps in safe custody, controls or administers trust property	Lender against the security of securities
An estate agent	Financial service providers excluding those registered to provide advice and or intermediary services in short term insurance or health service benefits.
An authorised user of an exchange	Persons who issue, sell or redeem travelers' cheques, money orders or similar instruments
Collective Investment Scheme managers	Postbank
A bank or mutual banks	The Ithala Development Finance Corporation Limited
Long-term insurer	A money remitter
Gambling licensee	

Reporting institutions are any person who carries on the business of dealing in motor vehicles or in Kruger Rands.

1.4 Registration by institutions

Every accountable institution and every reporting institution must, within the prescribed period and in the prescribed manner, register with FIC, accompanied by such particulars as FIC may require.

A registered accountable institution or reporting institution must notify FIC, in writing, of any changes to the particulars furnished within 90 days after such a change.

FIC keeps and maintains a register of every accountable institution and reporting institution registered with them.

1.5 Risk-based approach

FICA requires accountable institutions to apply a risk-based approach when carrying out client due diligence measures.

1.5.1 The concept of risk

According to international best practice risk rating methodology, risk refers to the likelihood and impact of uncertain events on set objectives. The impact can be either a positive or negative deviation from what is expected. This uncertainty is a function of three factors:

- **Threat:** A threat is a person or group of people, object or activity with the potential to cause harm. In the context of money laundering and terrorist financing this includes criminals, terrorist groups and their facilitators, their funds, as well as the past, present and future money laundering or terrorist financing activities.
- **Vulnerability:** The concept of vulnerabilities comprises those things that can be exploited by the threat or that may support or facilitate its activities. Identifying vulnerabilities, as distinct from threats, means focusing on, for example, the factors that represent weaknesses or features that may be exploited in a given system, institution, product, service etc. The areas in which these vulnerabilities may arise are discussed in more detail later in this guidance.
- **Consequence:** Consequences refer to the impact of a threat or the exploitation of vulnerability if this impact is to materialise.

The context of the above is important. For example, “threat" or “consequence” to whom or what. On the other hand, vulnerability could arise from external and internal factors and may be either controllable or uncontrollable.

Risk in the context of money laundering or terrorist financing can therefore be thought of as the likelihood and impact of money laundering or terrorist financing activities that could materialise as a result of a combination of threats and vulnerabilities manifesting in an accountable institution.

1.5.2 Money laundering and terrorist financing (ML/TF) Risks

The concept of ML/TF risks, as the term implies, relate to threats and vulnerabilities that may promote the laundering of proceeds of unlawful activities or the financing of terrorism, on the one hand, or may jeopardise the detection, investigation or prosecution of these activities or the possibility of the forfeiture of proceeds of unlawful activities, on the other.

On a national level these are threats and vulnerabilities which put at risk the integrity of South Africa's financial system and negatively impacts the administration of criminal justice which affects the safety and security of South Africans as well as that of people outside of South Africa.

In relation to accountable institutions, ML/TF risks are threats and vulnerabilities which put the accountable institution at risk of being abused in order to facilitate ML/TF activities. These relate to the potential that clients, by using the accountable institution's products and services, can exploit the accountable institution to promote money laundering or terrorist financing activities.

The nature of these risks relate to a number of aspects, including the features of the intended target market of clients who are likely to use an accountable institution's range of products and services, the geographic locations of an accountable institution's operations and of its clients, the delivery channels through which persons become clients of an accountable institution or through which clients access its products and services, the features of a particular product or service, etc.

In order to have a robust ML/TF risk management system, accountable institutions must be able to demonstrate how they contextualize the concepts of "ML/TF risk" within their particular businesses as having an impact on their operational, line management and strategic objectives. Controls should be purposefully built and/or adapted to address ML/TF risks.

1.5.3 Risk rating

Risk-rating implies assigning different categories to different levels of risk according to a risk scale and classifying the ML/TF risks pertaining to different relationships or client engagements in terms of the assigned categories. As no two accountable institutions are the same, the level of risk and therefore the risk ratings attributed to particular business relationships or other engagements with clients may vary between accountable institutions.

A risk scale should be tailored according to the size of the accountable institution and consideration may be given to criteria set out in international best practice. The complexity of the risk scale should reflect the size and complexity of the accountable institution and the nature and the range of products and services it offers to its clients.

The ML/TF risk associated with a particular client engagement is not static. The factors underlying any given risk-rating will inevitably change over time. It is therefore essential that accountable institutions re-evaluate the relevance of particular risk factors and the appropriateness of previous risk-ratings from time to time and determine the intervals at which this will be done.

Accountable institutions must document the risk-rating methodology and procedures which they apply as well as the conclusions reached through the processes in the accountable institution's RMCP. This includes the criteria and the intervals for the re-evaluation of risk-ratings.

1.5.4 Risk mitigation

Risk mitigation in the context of ML/TF refers to the activities and methods used by an accountable institution to control and minimise the ML/TF risks it has identified. An accountable institution should therefore apply its knowledge and understanding of its ML/TF risks in the development of control measures to mitigate the risks identified.

The risk assessment process will therefore assist accountable institutions in determining the nature and extent of resources necessary to mitigate identified risks.

Institutions should use the client due diligence process as one of the measures to mitigate the ML/TF risk associated with a proposed business relationship or single transaction. The client due diligence process provides an accountable institution with the information required to know who they are doing business with, to know who benefits from the business it does with its clients, to understand the nature of the business it does with its clients and to determine when the business with clients should be considered suspicious or unusual. This is one of the mechanisms at accountable institutions' disposal to mitigate the risk of exploitation for money laundering or terrorist financing purposes.

An accountable institution's systems and controls should provide for more information to be obtained about their clients, more secure confirmation of clients' information to be applied and closer scrutiny to be conducted to their clients' transaction activities where they assess the risk of abuse to be higher. This is referred to as enhanced due diligence.

By the same token an accountable institution's systems and controls may allow for less information to be obtained, less secure confirmation of information to be applied and less frequent scrutiny to be conducted where they assess the risk of abuse to be lower. This is referred to as simplified due diligence.

An accountable institution should always have grounds on which it can base its justification for a decision that the appropriate balance was struck in a given circumstance.

The systems and controls by which an institution decides to manage ML/TF risks and the levels of due diligence it chooses to apply in relation to various risk levels must be documented in its Risk Management and Compliance Program (RMCP).

TOPIC 2 MAIN DUTIES IMPOSED ON ACCOUNTABLE INSTITUTIONS

LEARNING OUTCOMES

After studying the topic, the learner should be able to-

- Outline the main duties imposed on accountable institutions as prescribed by the Financial Intelligence Centre Act

2.1 Introduction

FICA requires that an accountable institution must comply with the following main duties:

- Customer due diligence.
- Keeping of records.
- Providing the Financial Intelligence Centre (FIC) Access to information.
- Reporting certain transactions and suspicious activities. (Applicable to reporting institutions as well)

The accountability and responsibility for the effective management of anti-money laundering procedures lies with the key individual and may be delegated to responsible employees.

2.2 Customer due diligence

FICA impose certain duties on accountable institutions regarding keeping record of business relationships and transactions. These duties become the duty of a representative associated with an FSP.

FICA stipulates that an accountable institution may not establish a business relationship or conclude a transaction with a client unless the accountable institution has taken the prescribed steps.

When an accountable institution engages with a prospective client to enter into a single transaction or to establish a business relationship, the institution must, in the course of concluding that single transaction or establishing that business relationship and in accordance with its Risk Management and Compliance Programme establish and verify the identity of the client.

If the client is acting on behalf of another person, the identity of that other person must be established and verified as well as the client's authority to conduct business on behalf of the other person.

If another person is acting on behalf of the client, the identity of the other person must be verified as well as the other person's authority to act on behalf of the client.

If an accountable institution had established a business relationship with a client before FICA took effect, a new transaction may not be concluded before all the above steps have been taken to identify all persons associated and before all accounts at the accountable institutions that are involved in transactions concluded during the business relationship are traced.

An accountable institution that does not adhere to these prescriptions is guilty of an offence.

2.2.1 Understanding and obtaining information on business relationship

When an accountable institution engages with a prospective client to establish a business relationship, the institution must, in addition to the steps verification of identity and in accordance with its Risk Management and Compliance Programme, obtain information to reasonably enable the accountable institution to determine whether future transactions that will be performed in the course of the business relationship concerned are consistent with the institution's knowledge of that prospective client, including information describing the following:

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

2.2.2 Additional due diligence measure relation to legal persons, trust and partnerships

This section applies in respect of a legal person, partnership or trust or a similar arrangement between natural persons, whether it is incorporated or originated in the South Africa or elsewhere.

If a client is a legal person or a natural person acting on behalf of a partnership, trust or similar arrangement between natural persons, an accountable institution must, in addition to verifying the identities and establishing the nature of the business relationship and in accordance with its Risk Management and Compliance Programme, establish the following:

- The nature of the client's business
- The ownership and control structure of the client.

If a client is a legal person, an accountable institution must in addition to verifying the identities and establishing the nature of the business relationship and in accordance with its Risk Management and Compliance Programme, establish the identity of the beneficial owner of the client by determining the identity of each natural person who, independently or together with another person, has a controlling ownership interest in the legal person.

If in doubt whether a natural person is the beneficial owner of the legal person or no natural person has a controlling ownership interest in the legal person, determining the identity of each natural person who exercises control of that legal person through other means. if a natural person is not identified, the accountable institution must establish the identity of each natural person who exercises control over the management of the legal person, including in his or her capacity as executive officer, non-executive director, independent non-executive director, director or manager.

If a natural person, in entering into a single transaction or establishing a business relationship is acting on behalf of a partnership between natural persons, an accountable institution must, in addition to verifying the identities and establishing the nature of the business relationship and in accordance with its Risk Management and Compliance Programme, establish the following:

- Establish the identifying name of the partnership, if applicable.
- Establish the identity of every partner, including every member of a partnership, an anonymous partnership or any similar partnership.

- Establish the identity of the person who exercises executive control over the partnership. Establish the identity of each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the accountable institution on behalf of the partnership.
- Take reasonable steps to verify the particulars obtained
- Take reasonable steps to verify the identities of the natural persons so that the accountable institution is satisfied that it knows the identities of the natural persons concerned.

If a natural person, in entering into a single transaction or establishing a business relationship is acting in pursuance of the provisions of a trust agreement between natural persons, an accountable institution must, in addition to verifying the identities and establishing the nature of the business relationship and in accordance with its Risk Management and Compliance Programme, establish the following:

- Establish the identifying name and number of the trust, if applicable.
- Establish the address of the Master of the High Court where the trust is registered, if applicable.
- Establish the identity of the founder.
- Establish the identity of each trustee and each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the accountable institution on behalf of the trust.
- Establish the identity of each beneficiary referred to by name in the trust deed or other founding instrument in terms of which the trust is created; or if beneficiaries are not referred to by name in the trust deed or other founding instrument in terms of which the trust is created, the particulars of how the beneficiaries of the trust are determined.
- Take reasonable steps to verify the particulars obtained and take reasonable steps to verify the identities of the natural persons so that the accountable institution is satisfied that it knows the identities of the natural persons concerned.

2.2.3 Ongoing due diligence

An accountable institution must, in accordance with its Risk Management and Compliance Programme, conduct ongoing due diligence in respect of a business relationship, which includes the following:

- Monitoring of transactions undertaken throughout the course of the relationship, including, where necessary the source of funds, to ensure that the transactions are consistent with the accountable institution's knowledge of the client and the client's business and risk profile; and the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent business or lawful purpose
- Keeping information obtained for the purpose of establishing and verifying the identities of clients up to date.

2.2.4 Doubts about veracity of previously obtained information

When an accountable institution, subsequent to entering into a single transaction or establishing a business relationship, doubts the veracity or adequacy of previously obtained information which the institution is required to verify, the institution must repeat the steps contemplated in accordance with its Risk Management and Compliance Programme and to the extent that is necessary to confirm the information in question.

2.2.5 Inability to conduct customer due diligence

An accountable institution must not establish a business relation or conclude a transaction or must terminate in accordance with its risk management and compliance programme an existing business relationship with a client, if an accountable institution is unable to:

- Establish and verify the identity of a client or other relevant person.
- Obtain the required information contemplated.

The accountable institution can also consider reporting the client under section 29 of FICA.

2.2.6 Single transaction threshold

FICA defines a single transaction as a transaction other than a transaction concluded in the course of a business relationship and where the value of the transaction is not less than R5 000.00 (the amount is determined by the Minister of Finance in the Regulations).

Therefore, accountable institutions are not required to carry out the full scope of CDD measures in respect of clients conducting single transactions below R5 000. These transactions can be described as occasional or once-off business where there is no expectation on the part of the accountable institution or the client that the engagements would recur over a period of time.

Institutions need to determine what constitutes a single transaction in the context of their particular business for purposes of complying with the obligations of FICA in as far as it applies to single transactions.

Accountable institutions are not required to carry out the full scope of CDD measures in respect of clients conducting single transactions below the value set by the Minister of Finance.

However, the threshold for single transactions does not apply to the obligations set out in section 20A of FICA. This means that, in spite of a single transaction being below the threshold, the accountable institution is still prohibited from dealing with an anonymous client or a client with an apparent false or fictitious name. As a result, in such cases, the accountable institution should obtain and record at least some information describing the identity of the client even if that information does not have to be verified. The manner in which the accountable institutions complies with section 20A of FICA in respect of business relationships and single transactions, both below and above the threshold, must be recorded in the institution's RMCP.

2.2.7 Foreign prominent public official

If an accountable institution determines in accordance with its Risk Management and Compliance Programme that a prospective client with whom it engages to establish a business relationship, or the beneficial owner of that prospective client, is a foreign prominent public official, the institution must do the following:

- Obtain senior management approval for establishing the business relationship.
- Take reasonable measures to establish the source of wealth and source of funds of the client.
- Conduct enhanced ongoing monitoring of the business relationship.

A foreign prominent public official is an individual who holds, who has help at any time in the preceding 12 months a prominent public function including that off the following:

- Head of State or head of a country or government.
- Member of a foreign royal family.
- Government minister or senior politician or leader of a political party.
- Senior judicial official.
- Senior executive of a state-owned corporation.
- High ranking member of the military.

2.2.8 Domestic prominent influential person

If an accountable institution determines that a prospective client with whom it engages to establish a business relationship, or the beneficial owner of that prospective client, is a domestic prominent influential person and that, in accordance with its Risk Management and Compliance Programme, the prospective business relationship entails higher risk, the institution must—

- Obtain senior management approval for establishing the business relationship.
- Take reasonable measures to establish the source of wealth and source of funds of the client.
- Conduct enhanced ongoing monitoring of the business relationship.

A domestic prominent influential person is an individual who holds, including in an acting position for a period exceeding six months, or has held at any time in the preceding 12 months, in the South Africa:

- A prominent public function including that of-
    - The President or Deputy President.
    - A government minister or deputy minister.
    - The Premier of a province.
    - A member of the Executive Council of a province.
    - An executive mayor of a municipality.
    - A leader of a political party registered in terms of the Electoral Commission Act.
    - A member of a royal family or senior traditional leader
    - The head, accounting officer or chief financial officer of a national or provincial department or government component

- The municipal manager of a municipality appointed in terms of section 54A of the Local Government: Municipal Systems Act.
- A chief financial officer designated in terms of the Municipal Finance Management Act.
- The chairperson of the controlling body, the chief executive officer, or a natural person who is the accounting authority.
- The financial set up a public entity to the Public Finance Management Act.
- The chairperson of the controlling body, chief executive officer, chief financial officer or the chief investment officer of a municipal entity.
- A constitutional court judge any other judge.
- An ambassador or high commissioner or other senior representative of a foreign government based in South Africa.
- An officer of the South African National Defense Force above the rank of major-general.

- Persons holding the following positions if a company provides goods or services to the state and the annual value of the goods or services exceeds an amount determined by the Minister:
  - Chairperson of the board of directors
  - Chairperson of the audit committee
  - Executive officer or chief financial officer
- The position of head, or other executive directly accountable to that head, of an international organisation based in the South Africa.

2.2.9 Family members and known close associates

The provisions relation to foreign and domestic prominent influential persons apply to immediate family members and known close associates of a person in a foreign or domestic prominent position, as the case may be.

Immediate family member includes the following:

- The spouse, civil partner or life partner.
- The previous spouse, civil partner or life partner, if applicable.
- Children and stepchildren and their spouse, civil partner or life partner
- Parents.
- Sibling and step sibling and their spouse, civil partner or life partner.

2.2.10 Impact of POPI on the identification and verification requirements

The processing of personal information of clients for the purposes of FICA compliance may only be done within the confines of the Protection of Personal Information Act, 2013 (the POPI Act).

While the processing and further processing of personal information of a client for purposes of FICA requirements is allowed in terms of the POPI Act, accountable institutions should be cautious of verifying clients' identities using third party data sources which may have obtained personal information about a client without the client's consent or knowledge.

2.2.11 Timing of verification

A client's identity and, where applicable, the identities of beneficial owners and other persons associated with a client, must be verified in the course of conducting a single transaction or entering into a business relationship. This means that an accountable institution may initiate the processes related to the conclusion of a single transaction or entering into a business relationship while it is verifying the relevant persons' identities, but the institution must complete the verification before the institution concludes a transaction in the course of the resultant business relationship or performs any act to give effect to the resultant single transaction.

This implies that accountable institutions may, for example, accept a mandate from a prospective client to establish a business relationship or to conclude a single transaction or take any similar preparatory steps with a view of establishing a business relationship or concluding a single transaction before completing verification of the identities of the prospective client and other relevant persons. However, in doing so accountable institutions must take care not to incur unmitigated ML/TF risks by, for example, receiving funds from a client which may have to be returned to the client before completing the verification or making funds available to a client before completing the verification.

The manner and processes for the identification of clients and verification of their identities described in an accountable institution's RMCP must also provide for the timing of verification and the mitigation of ML/TF risks where verification is not completed before a single transaction is conducted or a business relationship entered into.

2.3 Keeping of records

An accountable institution must keep the following due diligence records:

- Copies of, or references to, information provided to or obtained by the accountable institution to verify a person's identity.
- In the case of a business relationship, reflect the information obtained concerning-
    - The nature of that business relationship or transaction.
    - The intended purpose of the business relationship.
    - The source of the funds which the prospective client is expected to use in concluding transactions in the course of the business relationship.

An accountable institution must keep the following transaction records:

- The amount involved and the currency in which it was denominated
- The date on which the transaction was concluded.
- The parties to the transaction.
- The nature of the transaction.
- Business correspondence.
- If an accountable institution provides account facilities to its clients, the identifying particulars of all accounts and the account files at the accountable institution that are related to the transaction.

2.3.1 Maintenance of records under FICA

The following record keeping requirements are applicable in terms of FICA:

- Records may be kept in electronic format but must be capable of being reproduced in a legible format.
- Records may be kept by a third-party provider, providing that the accountable institution has free and easy access to the records and the records are readily available to the Centre and the relevant supervisory body for the purposes of performing its function. The Financial Intelligence Centre should also be provided with particulars of such third-party provider. Should the third party fail to keep proper records, the accountable institution is liable for that failure.
- An accountable institution must keep the records which relate to the establishment of a business relationship, for at least 5 years from the date on which the business relationship is terminated.
- An accountable institution must keep the records which relate to a transaction which is concluded for at least 5 years from the date on which transaction is concluded.
- An accountable institution must keep records relating to a transaction or activity which gave rise to a report for at least five years from the date on which the report was made.
- The records (or any extract thereof) are admissible as evidence before a Court.
- An accountable institution that does not adhere to these prescriptions is guilty of an offence.
- Any person who willfully tampers with these records kept or willfully destroy such records is guilty of an offence.

2.4 Access to information

An accountable institution must comply with a request by FIC to advice whether-

- A specified person is or has been a client of the institution.
- A specified person is acting or has acted on behalf of any client of the institution.
- A client of the accountable institution is acting or has acted for a specified person.
- Whether a number specified by the center was allocated by the accountable institution.

- On the type and status of a business relationship with a client of the accountable institution, reporting institution or person.

An accountable institution that fails to give assistance to a representative of the Financial Intelligence Centre is guilty of an offence.

2.4.1 Powers of access by authorized representative to the records in respect of reports required to be submitted to FIC

An authorised representative of FIC has access during ordinary working hours to any records kept by or on behalf of an accountable institution, and may examine, make extracts from or copies of, any such records for the purposes of obtaining further information in respect of a report made or ought to be made

The authorised representative of FIC may, except in the case of records which the public is entitled to have access to, exercise the powers by virtue of a warrant issued in chambers by a magistrate or regional magistrate or judge of an area of jurisdiction within which the records or any of them are kept, or within which the accountable institution conducts business.

A warrant may only be issued if it appears to the judge, magistrate or regional magistrate from information on oath or affirmation that there are reasonable grounds to believe that the records may assist FIC to identify the proceeds of unlawful activities or to combat money laundering activities or the financing of terrorist and related activities.

A warrant may contain such conditions regarding access to the relevant records as the judge, magistrate or regional magistrate considers appropriate.

An accountable institution must without delay give to an authorised representative of FIC all reasonable assistance necessary to enable that representative to exercise the powers.

2.5 Reporting certain transactions and suspicious activities

FICA imposes a duty on the FSP to report the following transactions:

- Cash transactions of more than R24 999.999 or an aggregate of smaller amounts which combine come to exceed this amount paid by the accountable institution or reporting institution to the client or a person on behalf of the client or received by the accountable institution or reporting institution from the client or a person acting on behalf of the client.
- Property associated with terrorist and related activities and financial sanction pursuant to the resolutions of the united nations security council.
- Suspicious and unusual transactions.

These transactions should be reported to the Money Laundering Reporting Officer of that FSP in the manner prescribed in the institution's internal rules.

The Money Laundering Reporting Officer will investigate the transaction to determine whether in fact the transaction was suspicious or unusual. If so, the Money Laundering Reporting Officer must report the transaction to the Financial Intelligence Centre within 2 days.

FIC may request additional information relation to the transactional activity and supporting documentation, concerning the report. The institution must furnish FIC in the prescribed manner and period with the additional information.

An accountable institution, reporting institution or person required to make a report may continue with and carry out the transaction in respect of which the report is required to be made unless FIC directs the accountable institution, reporting institution or person not to proceed with the transaction. FIC can direct the institution to not continue with the transaction for not longer than 10 working days.

2.5.1 Nature of a suspicion

In addition to circumstances where a person has actual knowledge, the reporting obligation under Section 29 of FICA also applies in circumstances where a mere suspicion may exist.

FICA does not define what constitutes a suspicion. The ordinary meaning of this term includes the state of mind of someone who has an impression of the existence or presence of something, or who believes something without adequate proof, or the notion of a feeling that something is possible or probable. This implies an absence of proof that a fact exists.

With this in mind, the starting point to considering whether circumstances give rise to a suspicion would be when those circumstances raise questions or gives rise to discomfort, apprehension or mistrust.

FICA adds an element of objectivity to this with the phrase *"ought reasonably to have known or suspected"* in Section 29 (1). The application of this phrase is explained in Section 1(3) of the POCA Act. Section 1(3) of the POCA provides that a person ought reasonably to have known or suspected a fact if a reasonably diligent and vigilant person with the same knowledge, skill, training and experience, as well as the knowledge, skill, training and experience that may reasonably be expected of a person in the same position, would have known or suspected that fact. This expands the scope of the obligation to identify circumstances which may indicate that a set of circumstances concerning a business, or the transactions involving the business, is of a suspicious nature.

When considering whether there is a reason to be suspicious of a particular situation, one should access all the known circumstances relating to that situation. This includes the normal business practices and systems with the industry where the situation arises.

A suspicious situation may involve several factors that may, on their own, seem insignificant, but taken together, may raise suspicion concerning that situation. The context in which a situation arises therefore, is a significant factor in assessing suspicion. This will vary from business to business and from client to client.

A person to whom Section 29 of FICA applies, should evaluate matters concerning the business in question and transactions involving the business, in relation to what seems appropriate and is within normal practices in the particular line of business of that person, and bring to bear on these factors such as the knowledge the person may have of the client. This should involve an application of persons knowledge of the client's business, financial history, background and behavior.

A particular category of transactions that are reportable u are transactions to which a person knows or suspects to have no apparent business or lawful purpose. This refers to situations where clients enter into transactions that appear unusual in a business context or where it is not clear that the purpose of the transaction(s) is lawful. In order to identify a situation where clients wish to engage in these unusual transactions, a person would have to have some background information as to the purpose of a transaction and evaluate this against several factors, such as the size and complexity of the transaction, as well as the person's knowledge of the client's business, financial history, background and behaviour.

In the subsections following more information is given as to factors that may indicate that a transaction is suspicious in a money laundering and terrorist financing context, respectively. These are indicators as to circumstances that may give rise to a suspicious state of mind or may be indicative of the fact that a reasonably diligent and vigilant person may have become suspicious of a particular transaction or series of transactions.

(I) Unusual business

The following unusual business transactions might be seen as suspicious:

- Deposits of funds with a request for their immediate transfer elsewhere.
- Unwarranted and unexplained international transfers.
- The payment of commissions or fees that appear excessive in relation to those normally payable.
- Lack of concern about high commissions, fees, penalties etc. incurred as a result of a particular method of transacting.
- Transactions that do not appear to be in keeping with normal industry practices.
- Purchase of commodities at prices significantly above or below market prices.
- Unnecessarily complex transactions.

- Unwarranted involvement of structures such as trusts and corporate vehicles in transactions.
- A transaction that seems to be unusually large or otherwise inconsistent with the clients financial standing or usual pattern of activities.
- Buying or selling securities with no apparent concern for making a profit or avoiding a loss.
- Unwarranted desire to involve entities in foreign jurisdictions in transactions.

(II) Unusual behaviour

The following behaviour might be seen as suspicious:

- A client who attempts to convince an employee not to complete any documentation required for the transaction.
- A client who makes inquiries that would indicate a desire to avoid reporting.
- A client who has unusual knowledge of the law in relation to suspicious transaction reporting.
- A client who seems very conversant with money laundering or terrorist activity financing issues.
- A client who is quick to volunteer that funds are clean and not being laundered.

(III) Suspicious identification

The following circumstances relating to identification might be seen as suspicious:

- The use of a seemingly false identity in connection with any transaction, including the use of aliases and a variety of similar, but different addresses and, in particular, the opening or operating of a false name account.
- Opening accounts using fictitious documents.
- A client who provides doubtful or vague identification information.
- A client who refuses to produce personal identification documents.
- A client who changes a transaction after learning that he must provide a form of identification.
- A client who only submits copies of personal identification documents.

- A client who wants to establish identity using something other than his or her personal identification documents.
- A client whose supporting documents lack important details such as contact particulars.
- A client inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.

2.5.2 Reactive reporting

Reactive reporting refers to the submitting of a suspicious transaction report to the Financial Intelligence Centre following an external prompt with a prior suspicion having been formed on the basis of the circumstances in which a particular transaction or series of transactions have been conducted. Examples of the prompts that may give rise to reactive reporting are as follows:

- Receiving a subpoena in terms of Section 25 of the Criminal Procedure Actor a similar process to provide evidence concerning matters relating to its business dealings with a particular client.
- Receiving a request to confirm whether a person is a client of the accountable institution in Terms of Section 27 of FICA in respect of a particular client.
- Receiving an Intervention Order in terms of Section 34 of FICA in connection with a transaction involving a particular client.
- Receiving a Monitoring Order in terms of Section 35 of FICA concerning the transactions of a particular client.
- Receiving other types of enquiries from government agencies such as investigating authorities or the South African Revenue Service about a particular client.
- Seeing information in the media that may adversely affect a particular client.

With regard to these external factors it is important to bear in mind that the obligation to file a STR with FIC arises where a person becomes aware of certain facts or in situations which should give rise to a suspicion. External factors such as those referred to here, may contribute to the forming of a suspicion, but in all cases these factors should be considered in conjunction with all other factors pertaining to a particular transaction or series of transactions. These factors should, not in and of themselves, form the reason for submitting a report to FIC in absence of any suspicion formed.

2.5.3 Legal protection of a reporter

Section 38 of FICA protects persons who participate in making reports to FIC. No legal action, whether criminal or civil, can be instituted against any natural or legal person who complies in good faith with the reporting obligations of FICA

In addition to protection against legal liability, FICA also protects the identities of those involved in making a report to FIC.

A person involved in making a report cannot be forced to give evidence in criminal proceedings concerning such a report. However, such a person may choose to do so voluntarily. If a person elects not to testify, no evidence regarding that person's identity is admissible as evidence in criminal proceedings.

2.6 Notification of persons and entities identified by Security Council of the United Nations

2.6.1 Introduction

FICA places the responsibility to administer the targeted financial sanctions (TFS) measures adopted by the United Nations Security Council (UNSC) in its Resolutions on the Financial Intelligence Centre (FIC).

Member countries are required to implement the targeted financial sanctions proposed by the UNSC in the context of combating the financing of the proliferation of weapons of mass destruction.

Sanctions impose restrictions on activities that relate to particular countries, goods and services, or persons and entities. TFS measures generally restrict sanctioned persons and entities from having access to funds and property under their control and from receiving financial services in relation to such funds and property. In order for these sanctions to be given effect FICA requires accountable institutions to freeze property and transactions pursuant to financial sanctions imposed in the UNSC Resolutions.

2.6.2 Mechanisms for implementation

Mechanisms for the implementation of the UNSC Resolutions include the publication in the Government Gazette by the Minister of Finance of a Notice of the adoption of the UNSC Resolution, and the publication of a Notice by the Director of FIC of persons who are subject to the sanction measures (the sanctions list). These Notices may be revoked if it is considered that they are no longer necessary to give effect to the applicable UNSC Resolutions. Otherwise the sanctions announced in these Notices remain in effect indefinitely.

The Notices by the Minister of Finance and the Director are public statements and are meant to advise both sanctioned persons and entities and accountable institutions who may have them as clients or prospective clients of the relevant sanctions. If an accountable institution has a sanctioned person or entity as a client, it is allowed to draw the attention of the person or entity to the relevant sanctions' notices.

The acquisition, collection or use of the property of persons or an entity whose names appear in the sanctions is prohibited. This includes the provision of financial services and products to those persons or entities.

In short this means that accountable institutions are not allowed to transact with a sanctioned person or entity or to process transactions for such a person or entity. The status quo as at the time of the imposition of the sanction in relation property or funds of the sanctioned person or entity must be maintained and no financial services may be provided to the person or entity.

The only exception to this general prohibition is in specific instances where the Minister of Finance has permitted certain financial services or dealings with property as discussed below.

Accountable institutions must report to FIC, the property in the accountable institution's possession or under its control which is owned or controlled by or on behalf of a person or an entity identified in the sanctions list.

2.6.3 Screening

FIC will maintain an updated sanctions list which will be available on its website and which will reflect available identity particulars of persons and entities contained in notices published by the Director.

Accountable institutions must be able to determine whether they have a sanctioned person or entity as a client or whether a prospective client is a sanctioned person or entity in order to determine their exposure to TFS-related obligations.

This implies that accountable institutions which are likely to come into contact with Sanctioned persons or entities are able to screen clients and prospective clients against the relevant sanctions lists. This should be done during the client-take-on process as well as subsequently as and when the UNSC adopts new TFS measures or expand existing ones.

Accountable institutions must therefore determine the likelihood that their client base and intended target market may include sanctioned persons or entities. This should assist the accountable institution in determining the amount of effort and resources it requires in order to determine whether they have sanctioned persons or entities as a client or whether prospective clients are sanctioned persons or entities. Accountable institutions that have business relationships with foreign persons and entities are more vulnerable to dealing with sanctioned persons and entities.

Accountable institutions should be mindful of the fact that failure to comply with TFS obligations is a criminal offence. The fact that an accountable institution had relied on a commercially available screening capability or that it had considered the risk of being exposed to TFS-related obligations to be low, would not be a defense against such a criminal charge.

2.6.4 Basic living expenses

FICA allows the Minister of Finance to permit a sanctioned person or entity to conduct financial services or deal with property affected by a sanction in order to allow such a person or entity access to certain basic living expenses. The permission of the Minister of Finance may contain the exact details of the types of expenses which may be met from the property that is affected by a sanction, the amounts of such expenses, the funds or property from which such expenses may be met and the conditions to the access to the relevant funds or property.

The Minister of Finance may also permit the provision of financial services or the dealing in affected property which are not related to providing for basic living expenses, but which are necessary in the normal course of business e.g. allowing for the accrual of interest or other earnings or are necessary in order to avoid prejudice to third parties.

As in the case of basic living expenses, the permission of the Minister of Finance may contain the exact details of the services, payments etc. that are permitted and the conditions thereto.

The permission of the Minister of Finance is granted by means of written communication with the sanctioned person or entity. The Director of FIC must give notice of the permission of the Minister of Finance to accountable institutions and others who may have an interest therein. This is done by means of publishing notices containing the permission of the Minister of Finance and the conditions thereto on FIC's website.

2.7 Prohibition against informing a client that a report has been made

A person that made a report or is about to make a report or who knows or suspects that a report was or is to be made, may not disclose the fact that the report was made or the contents of the report to any other person i.e. the client must not be tipped-off. This obviously includes the person about which the report is made.

FICA allows the reporter to disclose information under the following circumstances:

- If it is within the power and duties of that person in terms of any legislation.
- For carrying out the provisions of FICA.
- For legal proceedings (including proceedings before a judge in chambers).
- In terms of an order of court.

TOPIC 3 MEASURES TO PROMOTE COMPLIANCE BY ACCOUNTABLE INSTITUTIONS

LEARNING OUTCOMES

After studying the topic, the learner should be able to-

- Outline the measures imposed on an accountable institution to promote compliance with the Financial Intelligence Centre Act.

3.1 Introduction

The Financial Intelligence Centre Act (FICA) requires accountable institutions to develop, document, maintain and implement a risk management plan and compliance program as well as provide staff with training to promote compliance with regards to duties imposed by FICA.

3.2 Risk management plan and compliance program

An accountable institution must develop, document, maintain and implement a risk management plan and compliance program that provides for the following:

- The establishment and verification of identities.
- The information that must be recorded and kept.
- The manner and place in which such records must be kept.
- The steps to be taken to determine when a transaction is reportable.
- Such matters as may be prescribed by the Financial Intelligence Centre.

The risk management plan and compliance program must-

- Enable the accountable institution to identify, assess, monitor, mitigate and manage the risk that the provision by the accountable institution of products or services may involve or facilitate money laundering activities or the financing of terrorist and related activities.

- Provide the way the institution determines if a person is a prospective client in the process of establishing a business relationship or entering into a single transaction with the institution.
- Provide the way the accountable institution may not establish a business relationship or conclude a single transaction with an anonymous client or a client with an apparent false or fictitious name.
- Provide the way and the processes by which the establishment and verification of the identity of persons whom the accountable institution must identify is performed in the institution.
- Provide the way the institution determines whether future transactions that will be performed in the course of the business relationship are consistent with the institution's knowledge of a prospective client.
- Provide the way and the processes by which the institution conducts additional due diligence measures in respect of legal persons, trust and partnerships.
- Provide the way and the processes by which ongoing due diligence and account monitoring in respect of business relationships is conducted by the institution.
- Provide the way the examining of complex or unusually large transactions; and unusual patterns of transactions which have no apparent business or lawful purpose, and keeping of written findings relating thereto, is done by the institution.
- Provide the way and the processes by which the institution will confirm information relating to a client when the institution has doubts about the veracity of previously obtained information.
- Provide the way and the processes by which the institution will perform the customer due diligence requirements during the course of a business relationship, if the institution suspects that a transaction or activity is suspicious or unusual.
- Provide the way the accountable institution will terminate an existing business relationship.
- Provide the way and the processes by which the accountable institution determines whether a prospective client is a foreign prominent public official or a domestic prominent influential person.
- Provide the way and the processes by which enhanced due diligence is conducted for higher-risk business relationships and when simplified customer due diligence might be permitted by the institution.
- Provide the way and place at which the records are kept.

- Enable the institution to determine when a transaction or activity is reportable to the Centre.
- Provide for the processes for reporting information to the Centre.
- Provide the way the Risk Management and Compliance Programme is implemented in branches, subsidiaries or other operations of the institution in foreign countries so as to enable the institution to comply with its obligations under this Act.
- Provide the way the institution will determine if the host country of a foreign branch or subsidiary permits the implementation of measures required under this Act.
- Provide the way the institution will inform the Centre and supervisory body concerned if the host country does not permit the implementation of measures required under this Act.
- Provide for the processes for the institution to implement its Risk management and Compliance Program
- Provide for any other prescribed matter.

An accountable institution must indicate, in its Risk Management and Compliance Programme, if any of the above is not applicable to that accountable institution and the reason why it is not applicable.

The board of directors, senior management or other person or group of persons exercising the highest level of authority in an accountable institution must approve the Risk Management and Compliance Programme of the institution.

An accountable institution must review its Risk Management and Compliance Programme at regular intervals to ensure that the Programme remains relevant to the accountable institution's operations and the achievement of the requirements.

The risk management plan and compliance program must be made available to all employees involved in transactions. An accountable institution must on request make a copy of this risk management plan and compliance program available to the Financial Intelligence Centre or any supervisory body which performs regulatory or supervisory function in respect of the accountable institution e.g. the Financial Sector Conduct Authority.

3.3 Governance of anti-money laundering and counter terrorist financing compliance

The board of directors of an accountable institution which is a legal person with a board of directors, or the senior management of an accountable institution without a board of directors, must ensure compliance by the accountable institution and its employees with the provisions of this Act and its Risk Management and Compliance Programme.

An accountable institution which is a legal person must have a compliance function to assist the board of directors or the senior management, as the case may be, of the institution in discharging their obligations and must assign a person with sufficient competence and seniority to ensure the effectiveness of the compliance function.

The person or persons exercising the highest level of authority in an accountable institution which is not a legal person must ensure compliance by the employees of the institution with the provisions of FICA and its Risk Management and Compliance Programme, in so far as the functions of those employees relate to the obligations of the institution.

An accountable institution which is not a legal person, except for an accountable institution which is a sole proprietor must appoint a person or persons with sufficient competence to assist the person or persons exercising the highest level of authority in the accountable institution in discharging their obligation.

3.4 Training and monitoring of compliance

An accountable institution must provide training to its employees to enable them to comply with the provision of the Financial Intelligence Centre Act (FICA) and the Risk management plan and compliance program. The accountable institution must also appoint a person with the responsibility to ensure compliance by employees with FICA and the internal rules as well as compliance of the accountable institution with FICA.

TOPIC 4 ADMINISTRATIVE SANCTIONS AND PENALTIES

LEARNING OUTCOMES

After studying the topic, the learner should be able to-

- Outline the administrative sanctions and penalties that can be imposed on accountable and reportable institutions in terms of the Financial Intelligence Centre Act.

4.1 Administrative sanctions

FIC or a supervisory body may impose an administrative sanction on any accountable institution, reporting institution or other person to whom FICA applies when satisfied on available facts and information that the institution or person:

- Has failed to comply with a provision of FICA or any order, determination or directive made in terms of FICA.
- Has failed to comply with a condition of a license, registration, approval or authorisation issued or amended.
- Has failed to comply with a directive issued.
- Has failed to comply with a non-financial administrative sanction imposed in terms of this section.

FIC or a supervisory body may impose any one or more of the following administrative sanctions:

- A caution not to repeat the conduct which led to the non-compliance.
- A reprimand
- A directive to take remedial action or to make specific arrangements.
- The restriction or suspension of certain specified business activities
- A financial penalty not exceeding R10 million in respect of natural persons and R50 million in respect of any legal person.

Administrative sanctions will be given for the following:

- Failure to identify persons.
- Failure to comply with a duty in regard to customer due diligence.
- Failure to keep records.
- Failure to comply with direction of FIC.
- Failure to comply with duty in respect of Risk Management and Compliance Programme.
- Failure to register with FIC.
- Failure to comply with duty in regard to governance.
- Failure to provide training.
- Failure to comply with directives of FIC or supervisory body.

4.2 Penalties

In terms of FICA, two maximum penalties can be rewarded for the different offences:

- Maximum penalty of R100 million- or 15-years' imprisonment can be awarded for the following:
    - Destroying or tampering with records.
    - Failure to give assistance to representative of FIC.
    - Contravention of prohibitions relating to persons and entities identified by Security Council of United Nations.
    - Failure to provide FIC with requested information.
    - Failure to report cash transactions as prescribed.
    - Failure to report suspicious or unusual transactions.
    - Failure to report property associated with terrorist and related activities and financial sanctions pursuant to Resolutions of United Nations Security Council.
    - Unauthorised disclosure.
    - Failure to report conveyance of cash or bearer negotiable instrument into or out of South Africa.
    - Failure to report electronic transfers.

- Failure to comply with request.
- Failure to comply with direction of FIC.
- Failure to comply with monitoring order.
- Misuse of information.
- Obstructing of official in performance of functions
- Conducting transactions to avoid reporting duties.
- Unauthorised access to computer system or application or data.
- Unauthorised modification of contents of computer system.

- Maximum penalty of R10 million- or 5-years' imprisonment can be awarded for the following:
  - Failure to send a report regarding the conveyance of cash or bearer negotiable instrument to FIC.
  - Offences relating to inspection.
  - Hindering or obstructing appeal board.
  - Failure to attend when summoned.
  - Failure to answer fully or truthfully.