INSETA PROVIDER # 130299

COMPLIANCE AND LEARNING CENTER
THE EXPERT ACADEMY

Registration nr:	2018/242685/07
Vat nr:	40470281904
Office Tel:	010 597 0835
Admin WhatsApp:	068 127 0421
CEO WhatsApp:	083 821 8801
CEO Email:	anna@virtualclc.co.za
Website:	www.virtualclc.co.za
Address:	14 Vermooten Str Brackenhurst Alberton

Anti-Money Laundering & Terrorist Financing Training Reference Guide

© Compliance & Learning Center (Pty) Ltd
November 2022

Course summary

This course form parts of the training requirements imposed on accountable institutions in terms of the Financial Intelligence Centre Act.

The training is applicable to all employees as stipulated in the Risk Management compliance Program of NFS and training is to be undertaken at intervals stipulated in this policy document.

NFS is an accountable institution in terms of FICA.

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:** 60 minutes
- **Competency mark:** 70%

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 within 3 attempts.

Table of contents

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.
- Outline the main duties imposed on accountable institutions as prescribed by the Financial Intelligence Centre Act.
- Outline the measures imposed on an accountable institution to promote compliance with 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 pursues 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.

1.2.1 What is money laundering and terrorist financing?

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 very 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 providing 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	Post company
A bank or mutual bank	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 the Financial Intelligence Centre (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 Main duties imposed on accountable institutions

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

- Client 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 senior management who may delegate this responsibility to the Section 43 Compliance Officer and /or the Money Laundering Reporting Officer (MLRO).

1.5.1 Client due diligence

FICA impose certain duties on accountable institutions regarding keeping record of business relationships and transactions.

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, while 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.

(I) Understanding and obtaining information on business relationship

When an accountable institution engages with a prospective client to establish a business relationship, it 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 its' 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 during the business relationship concerned.

(II) 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, the accountable institution must identify 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.

(III) 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.

(IV) 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.

(V) Inability to conduct client due diligence

An accountable institution must not establish a business relationship or conclude a transaction if it unable to:

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

If an accountable institution is not able to complete the above, the existing relationship with the client may be terminated in accordance with its risk management and compliance programme. The accountable institution can also consider reporting the client under section 29 of FICA.

(VI) 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). This 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 to be 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 comply 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.

(VII) 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, it 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.

(VIII) 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, it 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 another executive directly accountable to that head, of an international organisation based in the South Africa.

(IX) Family members and known close associates

The provisions relating 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.

(X) 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.

(XI) 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.

1.5.2 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.

(I) 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 FIC 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.

1.5.3 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.

(I) 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.

1.5.4 Reporting certain transactions and suspicious activities

FICA imposes a duty on an accountable institution 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.

It is important to note that Section 29 of FICA refers to reports being made in connection with the proceeds of unlawful activities and money laundering, or terror financing offences as opposed to criminal activity in general. FICA therefore does not require reports to be made on suspected crimes or unlawful conduct by a person (apart from money laundering and terror financing activities).

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

In the case of suspicious transactions, the MLRO or the Head of Compliance 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 – called an intervention order.

One of the main purposes of an Intervention Order is to prevent the dissipation of funds or property which may be the proceeds of unlawful activity. A typical example of where this may be the case is where funds or assets are due to be transferred from one location to another or from one person to another, especially where the transfer will have the effect of moving the funds or assets out of South Africa. Reporters are encouraged to indicate to FIC at the time of making a report under Section 29 if they believe that the funds or assets involved in a transaction or series of transactions may be dissipated. The same also applies if a report has been filed with FIC and the reporter subsequently becomes aware that the suspected proceeds may be dissipated. In such cases the reporter may contact FIC quoting their reference number and informing FIC of the activities within such account.

(I) 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.

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.

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.

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.

(II) Reactive reporting

Reactive reporting refers to the submitting of a suspicious transaction report to the 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.

(III) 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.

1.6 Risk-based approach

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

1.6.1 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.

1.6.2 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 relates 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.

1.6.3 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.

1.6.4 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).

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

1.7.1 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.

1.7.2 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.

1.7.3 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 sanction's 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.

1.7.4 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.

1.8 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.

Contravening these prohibitions constitutes offences in terms of FICA that carry maximum penalties of imprisonment for a period of up to 15 years or a fine up to R10 million.

1.9 Measures to promote compliance by accountable institutions

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.

1.9.1 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.

An accountable institution's ability to apply a risk-based approach effectively is largely dependent on the quality of its RMCP. An accountable institution's RMCP must be sufficient for countering the ML/TF risks facing the institution. It is important for accountable institutions to bear in mind that a RMCP not only comprises of policy documents, but also of procedures, systems and controls that must be implemented within the institution. The RMCP can therefore be described as the foundation of an accountable institution's efforts to comply with its obligations under FICA on a risk sensitive basis.

The accountable institution's RMCP should also cover, among others the following:

- Appropriate training on money laundering and terrorist financing to ensure that employees are aware of, and understand, their legal and regulatory responsibilities and their role in handling criminal property and money laundering/terrorist financing risk management.
- Appropriate provision of regular and timely information to the board of directors or senior management relevant to the management of the institution's money laundering and terrorist financing risks.
- Appropriate documentation of the institution's risk management policies and risk profile in relation to money laundering and terrorist financing, including documentation of the institution's application of those policies.
- Appropriate descriptions of decision-making processes in respect of the application of different categories of CDD and other risk management measures, including escalation of decision-making to higher levels of seniority in the accountable institution where necessary.

- Appropriate measures to ensure that money laundering risks are considered in the day-to-day operation of the institution, including in relation to the following:
    - The development of new products.
    - The taking-on of new clients.
    - Changes in the institution's business profile.

An accountable institution must indicate, in its Risk Management and Compliance Programme, if any of the stipulations of FICA 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.

A RMCP should include a description of the board of directors' or senior management's accountability and the appointment of a person with adequate seniority and experience to assist with ensuring compliance with FICA. It is suggested that this description also indicate how the function to manage the establishment and maintenance of effective AML/CFT systems and controls is discharged in the accountable 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.

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

The board of directors or senior management must create a culture of compliance within the accountable institution, ensuring that the institution's policies, procedures, and processes are designed to limit and control risks of money laundering and terrorist financing and are fully consistent with the law and that staff adhere to them.

The board of directors or senior management should be fully engaged in decision making processes and take ownership of the risk-based measures adopted since they will be held accountable if the content of the RMCP (or its application in the accountable institution) is found to be inadequate.

An accountable institution 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.

1.9.3 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 RMCP.

1.10 Administrative sanction and penalties

1.10.1 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 client 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.

1.10.2 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.

TOPIC 2 CLIENT DUE DILIGENCE WITHIN NFS

LEARNING OUTCOMES

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

- Understand the risk-rating process of Intersure.
- Outline the process for establishing and verifying information
- Outline the process of due diligence for all type of transactions.
- Outline the process of ongoing client due diligence.
- Identify influential or exposed persons and follow the procedures in this regard.

2.1 Introduction

NFS is an accountable institution in their capacity as an FSP authorised in the long-term insurance product categories. NFS is not regulated under FICA in terms of short-term insurance product categories or health service product categories as such FSP's are not defined as accountable institutions.

Despite the above, all staff members are required to adhere to these internal rules and all members of staff are expected to:

- Be aware and follow these internal rules and legal requirements.
- Attend training initiatives and keep up to date on changes within the legislation and industry guidelines and procedures.
- Be alert to anything suspicious.
- Report suspicions and unusual transactions to the Money Laundering Reporting Officer.

Client identification and verification is a crucial part of any effective money laundering control system. NFS has a statutory obligation to establish and verify the identity of our clients.

This applies to every type of client, regardless of who they are, their personal status or the new type of service that they require. These requirements apply to all existing and new clients.

Each employee must report transactions concluded by him/her to the Reporting Officers where the necessary information was not obtainable from the client or where the client refused to disclose or submit the information required.

NFS may not establish a business relationship or conclude a single transaction with a client, a person acting on behalf of a client or a client acting on behalf of a person, unless NFS has taken the prescribed steps to identify and verify the client or the person and the person's authority to act. This also includes all business relationships that NFS had prior to the Act taking effect.

NFS adopted a risk-based approach while on-boarding its clients. The parameters of risk perception shall be defined in terms of nature of business activity, location of the entity and his/her clients, mode of payments, volume of turnover etc. to enable categorisation of clients into low, medium, and high risk. A risk-matrix shall be used to categories clients to grade the clients into low/medium/high risk categories.

NFS shall prepare a profile for each new client based on risk categorisation. The profile may contain information relating to client's identity, social/financial status, nature of business activity, information about the clients' business and their location etc.

2.2 Categorisation of clients according to risk

Clients are categorised according to risk relating to money laundering and terrorist financing. The categories are as follows:

- Low risk
- Medium risk
- High risk

2.2.1 Low risk clients

The following clients are considered low risk clients:

1. Current active clients where we also manage their Short-Term Portfolio (Commercial and/or Personal Short-Term Policies).
2. Whereby NFS clients have been active clients for more than three years.
3. Where all financial transactions are being processed via debit order.
4. Single need transactions (i.e., Risk Policy Only)

2.2.2 Medium risk clients

The following clients are considered medium risk clients:

1. Client whose Short-Term Policies are not managed by NFS.
2. New Clients.
3. Where clients do not transact via debit order.

4. Whereby more than on legal entity is involved (i.e., Trusts, Companies, Closed Corporations and Partnerships).
5. Multiple Cover (E.g., Invest and/or Pension additional to Life Cover)

2.2.3 High risk clients

The following clients are considered high risk clients:

1. Domestic Prominent Influential Persons as defined in Section 21G and Schedule 3A.
2. Foreign Prominent Public Official as defined in Section 21F and Schedule 3B.
3. Single cash transactions where the amount exceeds R25 000.00
4. Foreign Companies and Individuals.
5. Not having an active Commercial and/or Personal Short-Term Policy with NFS.

2.3 Procedure for client on-boarding

All Representatives of NFS are required to complete our FICA checklist for new business and reviews and provide the identification document for record keeping.

2.4 Client identification and verification

2.4.1 Categories of clients

The clients of NFS fall into the following categories:

- **Natural persons:** Natural persons include any of the following:
  - Citizens or residents of South Africa
  - Foreign nationals temporarily resident in South Africa
  - Foreign nationals not resident in South Africa
- **Legal Persons:** Legal persons include any of the following:
  - Close Corporation
  - South African Companies
  - Foreign Companies
  - Other legal persons, e.g., organs of State including Government departments, provident funds, pension funds etc.
- **Partnerships:** A partnership is a form of business enterprise. A partnership exists when there is a voluntary association of two or more persons engaged together for the purpose of doing lawful business as a partnership, for profit.

- **Trusts:** Means a trust as defined in section 1 of the Trust Property Control other than a trust stablished -
    - By virtue of a testamentary writing.
    - By virtue of a court order
    - In respect of persons under curatorship.
    - By the trustees of a retirement fund in respect of benefits payable to the beneficiaries of that retirement fund.

Additional due diligence needs to be undertaken in terms of foreign nationals and foreign companies

2.4.2 Acceptable documentation for verification

(I) Acceptable identity documents

South African Citizens

A valid green bar-coded identity document or smart ID card is accepted to verify the identity information. Valid means that the document must be current and unexpired.

If the client is a Company or a Trust, the relevant Identity Documents must be provided for all the Directors/Shareholder and Trustees.

Foreign nationals

Passport and if applicable independent confirmation from embassy.

Close corporations

Most recent versions of the founding Statement and Certificate of Incorporation (form CK 1) and amended Founding Statement (formCK2) if applicable is required to verify the information. The bearing stamp of the Registrar of Close Corporations must be present, and the must be signed by an authorised member of employee of the CC. In exceptional cases, where it is not possible to obtain the CK1 or CK2, electronic verification as provided for by the CIPC in the form of a Disclosure Certificate may be accepted.

South African companies

Most recent versions of Certificate of Incorporation (form CM 1). Notice of registered office and postal address (form CM 22) - bearing the stamp of the Registrar of Companies and signed by the company secretary. In exceptional cases, where it is not possible to obtain the CM1 or CM22, electronic verification as provided for by the CIPC in the form of a Disclosure Certificate may be accepted.

Foreign companies

Official document issued by an authority for recording the incorporation of the foreign company, witnessing its incorporation, and bearing name/number/address. Any document that can be reasonably expected to achieve such verification. After 01 May 2011 – Registration Certificate of External Company (CoR20.2) for foreign companies registered under South African Companies Act.

Other legal persons

Constitution or other founding document in terms of which the legal person is created.

(II) Proof of residence

Any of the following documents not more than 3 months' old reflecting the name or initials and surname of the client can be obtained to verify the proof of residence:

- Utility Bill (Municipal Water and Lights Account or Property Managing Agent Statement).
- Recent signed lease agreement/Property Agreement.
- Municipal rates and taxes invoice.
- Short term Insurance Schedule (including NFS Insurance Group).
- Letter from Accountant, Attorney or Bank Manager stating they have known the client for a period of 3 years & confirm the address.
- Verified Bank Statement.
- Valid TV License.
- Telephone or cellular telephone account.
- Face to face verification.

All Representatives of NFS are required to complete the FICA checklist and confirm (together with the face-to-face verification document) whether they consulted with the client at the client's home residence and provide the document for record keeping for all new and existing business.

(III) Income tax registration number if issued

No document is needed to verify the tax registration number.

(IV) Proof of bank account

NFS may only accept bank account verification that is less than three months old if/where applicable. Any one of the below valid documents reflecting the account number may be accepted:

1. Cancelled Cheque
2. Bank Statement with a bank stamp (no internet or credit card statements accepted)
3. A letter from the bank confirming banking details

2.4.3 On-boarding of new clients: Information to be established and verified

The following information must be established and verified on -on-boarding of new clients depending on the category of client.

(I) Natural persons: South African Citizens

The following information to be obtained and verified:

- The clients' full names.
- The clients' date of birth.
- The clients' proof of identity number.
- The clients' proof of physical home address.
- The income tax number, if such a number has been issued to the person.

All Representatives of NFS are required to complete the FICA checklist and provide the verification documentation for record keeping with regards to Individuals.

(II) Natural persons: Foreign nationals

The following information to be obtained and verified

- The clients' full names.
- The clients' date of birth.
- The clients' passport number.
- The clients' proof of physical home address.
- The income tax number, if such a number has been issued to the person.

If NFS requires further confirmation of a Foreign National, NFS may obtain a letter from a person of Authority (for example, from the relevant Embassy) which confirms authenticity of that person's identity document (Passport).

All Representatives of NFS are required to complete the FICA checklist and provide the verification document for record keeping with regards to Foreign Nationals.

(III) Legal persons: Trusts

The following information to be obtained and verified:

- Identify the name and number of the Trust.
- Copy of the Letter of Authority from the Master of the High Court where the Trust is registered.
- Income tax number.
- Trade name.
- Business address.
- Particulars of how beneficiaries of the Trust are determined.
- Full names, proof of identity number, date of birth of each Trustee of the Trust and of each natural person who purports to act on behalf of the Trust.

- Proof of Residential address and contact details of each Trustee, each person who purports to act on behalf of the Trust, and of the founder of the Trust.

All Representatives of NFS are required to complete the FICA checklist and provide the verification documentation for record keeping with regards to Individuals.

(IV) Legal persons: Partnerships

The following information to be obtained and verified:

- Registered name of the Partnership (verify using a Partnership Agreement).
- Business trading name.
- Registered business address.
- Registration number.
- Income tax number and VAT registration number.
- Name, proof of identity, date of birth and Proof of Residential address of each Partner, each person who exercises executive control over the Partnership, and of each person who can transact on behalf of the Partnership.

All Representatives of NFS are required to complete the FICA checklist and provide the verification documentation for record keeping with regards to Individuals.

(V) Companies and Closed Corporations

The following information to be obtained and verified:

- Registered name of the company or CC.
- Registration number of the business.
- Business trading name.
- Business address.
- The most recent Certificate of Incorporation (CM1) (company).
- Notice of Registered Office and Postal Address (CM22) (company).
- The most recent Founding Statement and Certificate of Incorporation (CK1) (Closed corporation).
- Income tax and VAT registration number (any SARS doc).
- Company - The full names, date of birth, residential address, contact particulars and identity number if the manager of the business as well as each person who can transact on behalf of the company. The full details of any natural person, legal person, partnership, or trust which holds more that 25% voting right in the company.
- Closed Corporation: The full names, date of birth, Proof of residential address, contact particulars and proof of identity number of each of the members and of any person who can transact of behalf of the business.

All Representatives of NFS are required to complete the FICA checklist and provide the verification documentation for record keeping with regards to Individuals.

(VI) Foreign companies

The following information to be obtained and verified:

- Incorporated Name, number, and address – An official incorporation document issued by the country of origin, bearing its name, incorporation number and business address.
- Trading name in the country where it conducts business.
- Trading name in the Republic.
- Operating address.
- Income tax number.
- VAT number.
- Full names, date of birth, proof of residential address, contact particulars and proof of identify number of the manager of the business as well as of each person who can transact on behalf of the company.
- The full details (as above) of any natural person, legal person, partnership, or trust who holds more than 25% voting of the company.

All Representatives of NFS are required to complete the FICA checklist and provide the verification document for record keeping with regards to Foreign Companies.

2.4.4 Acceptable document for third party verification

NFS must obtain from the person acting on behalf of another person information that provides proof of that person's authority to act on behalf of that other natural person, legal person, or trust. NFS must verify the information obtained by -

- Comparing the particulars of the natural or legal person, partnership or trust with information obtained by the accountable institution from, or in respect of, the natural or legal person, partnership, or trust in accordance with the as may be applicable.
- Establishing whether that information, on the face of it, provides proof of the necessary authorisation.

The following are examples of documents that may be accepted to confirm the authority of a person to act on behalf of another person and to confirm the particulars of the person authorising the third party to establish the relationship:

- Power of attorney.
- Mandate.
- Resolution duly executed by authorised signatories.
- A court order authorising the third party to conduct business on behalf of another person.

2.4.5 Legal incapacity

In the case the person does not have the legal capacity to establish a business relationship or conclude a single transaction without the assistance of another person, the following information in respect of that other person must be obtained:

- Full names.
- Date of birth.
- Identity number.
- Residential address.
- Contact particulars.

2.4.6 Verification in absence of contact person

If NFS obtained information about a natural or legal person, partnership, or trust without contact in person with that natural person, or with a representative of that legal person or trust, NFS must take reasonable steps to establish the existence or to establish or verify the identity of that natural or legal person, partnership, or trust, considering guidelines as per this Policy.

2.4.7 Inability to verify identity

If an employee is unable to establish and verify the identity of a client or other relevant person in, the employee must not establish a business relationship with a client or must terminate any existing business relationship with a client and consider making a Suspicious Transaction Report to the Financial Intelligence Centre.

NFS may not establish a business relationship with an anonymous client or client with an apparent false or fictitious name.

2.5 Beneficial owners and ultimate beneficial owners

In addition to establishing and verifying a legal person's identity, NFS shall also establish who the beneficial owner of the legal person is and will take reasonable steps to verify the beneficial owner's identity.

A beneficial owner is defined in respect of a legal person as a natural person who, independently or together with another person, owns the legal person, or exercises effective control of the legal person.

The Process of Elimination that NFS will follow to determine who the beneficial owner/ ultimate beneficial owner of a legal person is as follows:

- The process starts with determining who the natural person is who, independently or together with another person, has a controlling ownership interest in the legal person. The percentage of shareholding with voting rights is a good indicator of control over a legal person as a shareholder with a significant percentage of shareholding, in most cases, exercises control. In this context ownership of 25% or more of the shares with voting rights in a legal person is usually sufficient to exercise control of the entity.
- If the ownership interests do not indicate a beneficial owner, or if there is doubt as to whether the person with the controlling ownership interest is the beneficial owner, the accountable institution must establish who the natural person is who exercises control of the legal person through other means, for example, persons exercising control through voting rights attaching to different classes of shares or through shareholders agreements.
- If no natural person can be identified who exercises control through other means, the accountable institution must determine who the natural person is who exercises control over the management of the legal person, including in the capacity of an executive officer, non-executive director, independent non-executive director, director, or manager.

The methods that are used by NFS for establishing and verifying the identities of all natural persons will be used for establishing and verifying the identity/ties of the beneficial owner.

2.6 Enhanced due diligence (EDD)

NFS shall conduct one or more of any of the following additional enhanced due diligence checks on the medium and high-risk clients which include the natural and legal persons including partnerships and trusts.

The following are the enhanced due diligence measures taken:

- Each transaction is to be monitored comprehensively.
- Verification of FICA documentation
    - Medium risk clients: Every 3 years
    - High risk clients: Annually

The table following detail the additional documents that can sourced and verified if the situations so call for it according to risk category of client.

Figure 2.1: Additional documents that can be sourced and verified

Client type	Medium risk clients	High risk clients
Natural person	• Additional proof of source of income • Income tax Return	• Additional proof of source of income • Income tax Return
Legal persons	• Income tax Return • Adverse media check	• Income tax return • Financial statements • Adverse media check

2.6.1 Trigger of follow up enhanced due diligence

NFS has also identified the following triggers that will prompt a review of enhanced due diligence that was previously conducted. The review will be conducted by the representative and will be signed off by the money laundering report officer (MLRO) or the Head of Compliance:

- A review of a high-risk client's account activity and transaction behaviour shows that their level of Money laundering | terrorist financing risk remains high.
- A review of a low or medium risk client's account activity and transaction behaviour shows that their laundering | terrorist financing risk has increased since the previous assessment.
- Where there is negative media about the individual or entity, especially relating to financial irregularities or bribery and corruption.
- Where there is a drastic increase in the net worth of the client.
- There is a material change in the nature and purpose of the client's business relationship with NFS. A material change can be defined as a change in the nature and purpose of the client's business relationship that substantially and continually affects and increases the AML risk the client poses to NFS by continuing to maintain the business relationship.

2.7 Ongoing client due diligence

NFS shall apply its client identification, verification, and screening procedures to existing clients on the basis of materiality and risk, and should conduct due diligence reviews of such existing relationships at appropriate times as follows:

- Low risk clients: 5 years
- Medium Risk clients: 3 years
- High Risk clients: Annually

However, NFS shall undertake regular reviews of their existing client records in the event of the following:

- When a transaction of significance takes place.
- When there is a material change in the way the client interacts with NFS

If NFS becomes aware at any time that it lacks sufficient information about an existing client, it should take steps to ensure that all relevant client identification and verification information is obtained as quickly as possible.

If the client does not provide supporting documents that is required by the company within 20 business days from receipt of notice, the company will consider terminating the relationship.

2.8 Update of personal particulars of clients

NFS will endeavour to ensure that it maintains updated client information. However, at the time of on-boarding, the client is requested to advise the company if there is a change in her/her personal information.

2.9 Termination of existing companying relationship by company

NFS shall consider terminating the companying relationship with a client due to the following:

- Where the Company is unable to complete on-going client due diligence measures/formalities. This would pertain to circumstances where the client was on-boarded after all the client due diligence processes were completed but the Company was unable to perform on-going client due diligence.
- Where the risk profile of the client has changed, and the company has decided that the risk of continuing with the business relationship with the client is no longer aligned with the risk appetite of the company.

2.10 Influential or exposed persons

Enhanced due diligence as applicable to high-risk clients must be performed on the following categories of clients irrespective or risk rating:

- Politically exposed persons (PEPS)
- Foreign prominent public official.
- Domestic prominent influential persons.
- Any family member and known close associate of above.

The definitions of these persons according to FICA is considered in Topic 1

2.10.1 Process of enhanced due diligence to be followed for influential or exposed persons

NFS must adhere to the following process in this regard:

- All clients/beneficial owners to be checked through world-check screening system.
- If influential or exposed person status is obtained, get the PEP | FPPO | DPPO questionnaire completed by the client.
- Take reasonable measures to establish source of wealth and source of funds of client.
- Obtain approval from senior management for establishing business relationships with PEPs/ FPPOs/ DPIPs or a family member or close associate.
- Conduct enhanced ongoing monitoring of business relationship.

2.10.2 Change of client's status after on-boarding

NFS ensures that as part of its on-boarding process, all prospective clients are screened against both sanctions list as well as PEP and PIP lists using the world check database. Once the screening is completed, the clients are risk rated accordingly.

However, where a client's status changes after the on-boarding process have been completed, additional steps are taken by NFS if it is found that the client has become a PEP or PIP, or a family member or close associate of a PIP as defined in this RMCP.

NFS can identify the change in status either at the time of risk review of the relationship, at the time of database scrubbing or if the client has informed the company accordingly.

In instances where it has been confirmed that the client's status has changed to that of a high-risk profile, a risk review will be conducted, and the procedure indicated for PEPS/PIPS as detailed in this section will be followed.

The client will be marked as "high risk" and will be monitored accordingly until the termination of the business relationship.

2.10.3 Doubts about the veracity of previous obtain Information

Whenever circumstances arise where NFS, after entering into a single transaction or establishing a business relationship with an influential or exposed person and has doubts about the veracity of adequacy of previously obtained identification information, that accountable institution must repeat the steps to confirm the information in question.

TOPIC 3 REPORTING SUSPICIOUS TRANSACTIONS NFS PROTOCOL

LEARNING OUTCOMES

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

- Outline the procedure for reporting reportable transactions.
- Understand the requirements in terms of prohibition of letting a client know that a report has been made

3.1 Introduction

FICA imposes a duty on all representatives and staff mandated to NFS to report the following transactions:

1. Cash transactions above the cash threshold requirement or an aggregate of smaller amounts which combine come to exceed this amount.
2. Property associated with terrorist and related activities and financial sanction pursuant to the resolutions of the United Nations security council.
3. Suspicious and unusual transactions.
4. International funds transfers.

NFS does not deal with cash. All premiums and investment monies are paid to the collection entities and product suppliers. Therefore, reporting obligations 1 and 4 is not applicable to NFS.

No duty of secrecy or confidentiality or any other restriction on the disclosure or information, whether imposed by legislation or arising from the common law or agreement, affects compliance with reporting requirement to Financial Intelligence Centre of such nature.

3.2 Reporting

Each employee of NFS must immediately report a transaction to the Reporting Officer in the following events:

- Any cash transaction over the published threshold.
- Any unusual or suspicious transaction.
- When it was impossible for the employee to comply with the requirements in terms of FICA for whatever reason.
- Whenever in doubt as to whether to report to the Reporting Officer or not.

The responsibility to report a transaction in terms of FICA to the Financial Intelligence Centre will transfer from the employee to the Reporting Officer after a transaction was reported to the Reporting Officer. The Reporting Officer will determine and decide as to whether a transaction must be reported.

3.3 Reporting Officer

The Money Laundering, Control Reporting Officer for NFS is Hein Portwig, or any other person nominated on the GOAML System from time to time by the company.

If the employee has any questions or queries or is uncertain of any aspect relating to FICA, the employee must report to the Reporting Officer immediately before any transaction is finalized between the company and a client to ensure compliance with FICA.

The Reporting Officer has 2 days to report any suspicious transactions or activities to the Financial Intelligence Centre via the GOAML System.

Every Representative and Staff Member mandated by NFS must report to the Money Laundering Reporting Officer (MLRO) immediately of any suspicious activities.

3.4 Process for submitting STR's to the Centre

The Money Laundering Reporting Officer has a duty to submit all Suspicious Transaction Reports' (STR's) to FIC as prescribed by the GOAML System.

3.5 Prohibitions

NFS is absolutely prohibited in owning, dealing in, or otherwise benefitting from or making available, any property associated with any person against whom financial sanctions were imposed by the UN under Chapter VII and Section 26B.

A report regarding such a person must be made to FIC within the prescribed time.

3.6 Prohibition on letting a client know that a report has been made

NFS shall not disclose the fact such reporting or any information regarding the contents of any such report to any other person, including the person in respect of whom the report is or must be made, other than if it –

- Is within the scope of the powers and duties of that person in terms of any legislation.
- For the purpose of carrying out the provisions of FICA.
- To legal proceeding, including any proceedings before a judge in chambers; or
- In terms of an order of court.

3.7 Handling of clients' accounts after report has been made

All reports made to the concerned authority should be kept strictly confidential and should be handled only on a "need to know" basis. In addition, it is an offence to broadcast or publish any information which reveals that an STR has been made or the identity of anyone who has made a report.

NFS may continue with and carry out the transaction in respect of which the report is made unless the Financial Intelligence Centre or any such regulatory or supervisory body directs it not to proceed with the transaction.

3.8 Intervention by Financial Intelligence Centre:

If the Financial Intelligence Centre, after consulting NFS, has reasonable grounds to suspect that a transaction or a proposed transaction or a proposed transaction may involve the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities or may constitute money laundering, it may direct NFS, in writing not to proceed with the carrying out of that transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period as may be determined by Financial Intelligence Centre, which may not be more than 10 working days, in order to allow the Financial Intelligence Centre-

- To make the necessary inquiries concerning the transaction.
- To inform and advise an investigating authority or the National Director of Public Prosecutions if the Financial Intelligence Centre deems it appropriate.

TOPIC 4 RECORD KEEPING NFS PROTOCOL

LEARNING OUTCOMES

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

- List the records that must be kept in terms of FICA.
- Outline the record keeping protocol of Intersure in terms of FICA.

4.1 Introduction

Whenever NFS establishes a business relationship or concludes a transaction with a client, whether the transaction is a single transaction or concluded during a business relationship with the client, certain records must be maintained by NFS.

Records must be kept in such a format to allow easy access and retrieval by staff as required.

The economical, efficient, and secure management of records contained within each department is a responsibility shared by every employee.

Retention of records and management control measures and structures that are in place must be adhered to and in compliance with the Financial Service Providers supporting standards and procedures.

All personnel must be familiar and comply with NFS statements, policies, standards, and procedures.

To ensure compliance, NFS will monitor, test and audit relevant records and record storage systems for adequacy and compliance.

Non-compliance with, or violations of NFS retention of statements, policies, standards, and procedures could lead to disciplinary actions and/or legal proceedings, as defined in NFS standard Terms of Employment.

The Key Individual within NFS has the ultimate responsibility for the secure and proper retention of records across the company.

4.2 What records to be kept?

The records to be kept is considered in the subsections following.

4.2.1 Client Due Diligence records

NFS must keep record of all information pertaining to a client obtained during its processes to comply with the client due diligence requirements in terms of FICA. NFS shall keep record of the following:

- The identity of the client.
- If the client is acting on behalf of another person:
    - The identity of the person on whose behalf the client is acting
    - The client's authority to act on behalf of that other person.
- If another person is acting on behalf of the client:
    - The identity of that other person.
    - That other person's authority to act on behalf of the client.
- The way the identity of the persons was established.
- 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 during the business relationship.
- Any document or copy of a document obtained to verify a person's identity.

4.2.2 Transaction Records

NFS must keep a record of every transaction which it has concluded with a client. Transaction records must be sufficient to enable the transaction to be reconstructed. NFS must keep records of the following:

- The amount involved and the currency in which it was denominated.
- The parties to that transaction.
- the date on which the transaction was concluded.
- the nature of the transaction.
- Pertinent or relevant business correspondence.
- The identifying particulars of all accounts at the accountable institution that are involved in the transaction.
- All accounts that are involved in transactions concluded by that NFS during that business relationship.
- Record of single transactions.
- The name of the person who obtained the information referred to on behalf of NFS.

4.3 Period of maintenance of records

NFS must keep all required records for at least 5 years from the date on which-

- The business relationship is terminated.
- The transaction is concluded.
- A transaction or activity which gave rise to a report in terms of section 29 of FICA was submitted to the Financial Intelligence Centre.

NFS may keep its record in electronic form.

4.4 Records may be kept by third parties

NFS may keep the records with a third party if NFS has free and easy access to the records.

NFS is liable for any failure by the third party if the latter fails to properly comply with the requirements of record keeping as per FICA.

When such a third party is appointed to perform, the record keeping duties, NFS shall forth with provide the Financial Intelligence Centre with the following prescribed particulars regarding the third party:

- The third party's full name, if the third party is a natural person or registered name, if the third party is a close corporation or company.
- The name under which the third-party conducts business.
- The full name and contact particulars of the individual who exercises control over access to those records.
- The address where the records are kept.
- The address from where the third-party exercises control over the records.
- The full name and contact particulars of the individual who liaises with the third party on behalf of NFS concerning the retention of the records.

TOPIC 5 IMPLEMENTATION OF MEASURES TO PROMOTE COMPLIANCE BY NFS

LEARNING OUTCOMES

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

- Understand how the measure imposed by FICA to promote compliance is integrated within NFS.

5.1 Introduction

The Financial Intelligence Centre Act (FICA) requires NFS to develop, document, maintain and implement a Risk Management and Compliance Program as well as provide staff with training to promote compliance with regards to duties imposed by FICA. The governance structure of combating money laundering and terrorist financing activities must also be addressed by NFS.

5.2 Governance structure

The board of Directors (Charl de Vries and Hein Portwig) of NFS which is a legal person with a board of Directors, must ensure compliance by the NFS and its employees with the provisions of FICA and its Risk Management and Compliance Programme.

5.2.1 Anti-money laundering | counter-financing terrorist activities officer

NFS shall appoint an appropriately qualified anti-money laundering | counter-financing terrorist activities officer to have overall responsibility for the anti-money laundering | counter-financing terrorist function with the stature and the necessary authority within the company such that issues raised by this officer receive the necessary attention from senior management and business lines.

5.2.2 FICA compliance officer

The compliance officer is the person who is, in terms of FICA appointed by NFS with the purpose of overseeing compliance with FICA by NFS and its employees. In the registration process, is tasked with the duty to ensure that the details of NFS are correctly submitted on the Financial Intelligence Centre's website and that the registration process is finalized.

As an accountable institution, NFS must register one compliance officer only.

5.2.3 Money laundering reporting officer

A money laundering reporting officer (Money Laundering Reporting Officer) is envisaged to be a person, with the responsibility and authority to submit intelligence reports to FIC on behalf of the accountable or reporting institution.

The Money Laundering, Control Reporting Officer for NFS is Hein Portwig, or any other person nominated on the GOAML System from time to time by the company.

5.3 Risk management compliance programme

NFS has put into place a Risk Management and Compliance Programme (RMCP) which is to be followed by all employees. The RMCP enables NFS to identify, assess, monitor, mitigate and manage the risk that NFS is confronted with when providing products or services that may involve or facilitate money laundering or the financing of terrorist and related activities.

It also indicates how and what processes are followed by NFS when establishing and verifying the identity of a person as is required by FICA.

The RMCP details how ongoing due diligence is carried out by NFS in respect of all its clients.

The treatment of Politically Exposed Persons/Foreign & Domestic Prominent Public Officials are included in the RMCP so that NFS can adequately mitigate the risks involved when dealing with such categories of persons.

NFS's record keeping obligations as well as the relevant processes are also included in the RMCP.

The RMCP provides detailed guidelines on how transactions relevant for regulatory reporting are to be identified as well as the processes that are followed when a report is filed with the FIC.

5.4 Training of employees

One of the most important controls over the prevention and detection of money laundering is to ensure that employees are alert to the risks of money laundering and terrorist financing and are sufficiently trained in the identification of unusual activities or transactions which may prove to be suspicious.

NFS shall design its own training courses, seminars, training material or certificate courses dealing with FICA and the Regulations. Employees may be sent to attend external training programmes as and when the same are held in centers nearby to the branches. The Financial Intelligence Centre Act does however from time-to-time present awareness sessions to accountable institutions on the content of FICA and the relevant Regulations in conjunction with the relevant supervisory bodies. Such programmes may be attended by employees of NFS depending on need and convenience.

NFS will ensure that training is provided to all employees to enable them to comply with the provisions of FICA and of its Risk Management and Compliance Programme which are internal rules applicable to them.

NFS must establish from its risk frameworks perspective and business models the level of training to be provided to relevant staff members in terms of FICA. Different training programmes can be designed and implemented for the different levels of employees within the institution.

Employees that are not involved in the above activities may only require basic training. This shall include basic training on the relevant legislation, the internal rules, and procedures of NFS, and the more obvious warning signs in relation to money laundering.

NFS must provide training to the employees in any manner it deems appropriate. It shall be the responsibility of NFS to demonstrate that the training took place and that it was sufficient to enable the employees to understand and comply with FICA.

Employees will be required to successfully undergo an assessment once the training has been completed as per the NFS's Risk Management & Compliance Programme.

Such training will take place on an annual basis and an internal register maintained accordingly of subject being discussed and attendance.