DEVELOPMENT FINANCE CORPORATION LIMITED

BUSINESS FINANCE / PROPERTIES / TRANSACTIONAL SERVICES

FICA RISK MANAGEMENT AND COMPLIANCE PROGRAMME

IN TERMS OF SECTION 42 OF THE FINANCIAL INTELLIGENCE CENTRE AMENDMENT ACT, NO 38 OF 2001 (FICA)

Previous Review: July 2023	**Owner:** Group Risk
Date Created: **April 2018**	**Current Review:** June 2026
Number of Pages: 35	**Version:** 03
CONFIDENTIAL	
No part of this document may be disclosed verbally or in writing, including by reproduction, to any third party without the prior written consent of the Ithala Development Finance Corporation. This document, its associated appendices and any attachments remain the property of the Ithala Development Finance Corporation and shall be returned upon request.	

TABLE OF CONTENTS

1. DEFINITIONS

1.1 In this RMCP, the following words and expressions bear the meanings ascribed to them:

1.1.1 **"Accountable Institution"** Means any institution registered under schedule 1of FIC Act;

1.1.2 "**Anti-Money Laundering**" **(AML)** means the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

1.1.3 **"Business Relationship"** means an arrangement between the business and a client that contemplates a series of Transactions over a period;

1.1.4 **"Counter Terrorist Financing" (CTF)** means activities which involves the solicitation, collection and providing of funds and other assets with the intention that it may be used to support terrorist acts, terrorist organisations, or individual terrorists.

1.1.5 **"Cash"** means paper money, coins, or traveller's cheques.

1.1.6 **"CDD"** means the customer due diligence referred to in section 21 of FICA, which must be conducted in accordance with the procedures set out in FICA;

1.1.7 **"Client"** means a person who has mandated the business, where:

1.1.7.1 such person or its Counterparty has firmly indicated that it would like or is ready to transfer Value to the Business in giving effect to a single transaction or a business relationship.

1.1.8 **"Counterparty"** includes:

1.1.8.1 a purchaser in a sale agreement in respect of which the client is the seller, and *vice versa*; and

1.1.8.2 a lessee in a lease agreement in respect of which the client is the lessor, and *vice versa*; and

1.1.8.3 any other Counterparty in an agreement to which the client is a party.

1.1.9 '**Domestic Politically Exposed Person (DPEP)**' means a person referred to in Schedule 3A of the FIC Amendment Act (Act No. 38 of 2001) and as outlined under section 6.5 and 6.6 of this policy.

1.1.10 **"Employee"** means any estate agent acting as such within the IDFC (whether as a director, shareholder, member, manager, employee, or contractor), or any other client-facing staff member of the business, even if said staff member is not an estate agent.

1.1.11 "EDD" means enhanced due diligence.

1.1.12 **"FATF"** means the Financial Action Task Force (of which South Africa is a member), an international standard-setting body dedicated to combatting MLFT.

1.1.13 **"FIC"** means the Financial Intelligence Centre, a juristic person created under chapter 2 of FICA.

1.1.14 **"FICA"** means the Financial Intelligence Centre Act, No 38 of 2001, as amended from time to time.

1.1.15 **Foreign Politically Exposed Persons "FPEP"** means a person referred to in Schedule 3B of the FIC Amendment Act (Act No. 38 of 2001) and as outlined under 6.7 of this policy.

1.1.16 **"Governmental Authority"** means any public authority, and includes (without limitation):

1.1.16.1 the South African Revenue Service; and
1.1.16.2 the Commission for Intellectual Property and Companies; and
1.1.16.3 any organ of state.

1.1.17 **"ID"** means any document issued by a Governmental Authority that describes and identifies a natural person by his or her personal attributes, and which attributes must at least include his or her (i) forename and middle name (or initials), (ii) surname, (iii) unique identifying number, (iv) date of birth, and (vi) facial image. ID includes any of the following:

1.1.17.1 green, bar-coded South African identity document;
1.1.17.2 South African identity card (both sides);
1.1.17.3 Valid South African passport;
1.1.17.4 Valid South African driver's licence; and
1.1.17.5 Valid passport (Foreign Nationals).
1.1.17.6 Valid asylum seeker or refugee permit
1.1.17.7 Valid work permit

1.1.18 **"IDFC"** means Ithala Development Finance Corporation Limited.

1.1.19 **"Legacy Client"** is any person who had a business relationship with the IDFC before the Implementation date, and in respect of whom the business already has customer due diligence information as at the Implementation date, albeit in terms of the FICA dispensation that applied prior to this RMCP becoming effective.

1.1.20 **"MLFT"** means money laundering and the financing of terrorism, where "money laundering" refers to any practice through which the proceeds of crime are dealt with to obscure their illegal origins.

1.1.21 **"POCDATARA"** means the Protection of Constitutional Democracy Against Terrorism and Related Activities Act, No. 33 of 2004, as amended from time to time.

1.1.22 **"Prospective Client"** means a person who approaches the business to enlist the business' services, but that person or its Counterparty:

1.1.22.1 has not yet firmly indicated that it would like or is ready to transfer Value to the Business.

1.1.23 **"Compliance Officer"** means the person within the business charged with overseeing compliance with FICA and this RMCP.

1.1.24 **"RMCP"** means the Risk Management and Compliance Programme contained in this document, which has been designed in response to the business' obligations under section 42 of FICA;

1.1.25 **"Terrorist Activities"** means any of the offences specified in POCDATARA, all of which relate to terrorism;

1.1.26 **"Transaction"** means a transaction between the business and the client under which value will be transferred between the business on one hand, and the client, its principal or its representative, its Counterparty, or any other person for the client's account on the other hand.

2. RELATED LEGISLATION

2.1 FICA - Financial Intelligence Centre Act Number 38 of 2001(as amended)

2.2 NCA - National Credit Act Number 34 of 2005

2.3 ITHALA ACT - Ithala Act Number 5 of 2013

2.4 PFMA - The Public Finance Management Act Number 1 of 1999 as amended

2.5 Companies Act Number 71 of 2008

2.6 POCA - Prevention of Organised Crime Act Number 121 of 1998

2.7 POCDATARA - Protection of Constitution Democracy against Terrorist and Related Activities Act Number 23 of 2022

2.8 LRA- Labour Relations Act Number 66 of 1995 as amended

3. RELATED INTERNAL POLICIES, PROCEDURES AND CODES

3.1 Domestic Politically Exposed Persons (DPEP), Foreign Politically Exposed Persons (FPEP), and Prominent Influential Persons (PIP) Policy.

3.2 Enterprise Development Fund Investment Policy

3.3 IDFC Fund Investment Policy

3.4 Business Finance Standard Operating Procedures

3.5 Enterprise Risk Management Framework (ERM)

3.6 Fraud Prevention Plan

4. INTRODUCTION

Ithala Development Finance Corporation Limited, hereafter referred to as the IDFC, is an accounting institution listed under item 16 Schedule 1 to the Financial Intelligence Centre Act (FICA) and is registered with the FIC (Section 43B of the FIC Act) under the Organisation ID 24.

5. THE PURPOSE OF RMCP

Section 42 of the FICA places an obligation on accounting institutions to develop, maintain and implement a Risk Management Compliance Programme (RMCP) for anti-money laundering (AML) and Counter Terrorist Financing (CTF) to apply the risk-based approach to control Money Laundering/Financing Terrorist (ML/FT). The purpose of this RMCP is to provide clearly for the procedures, which must be followed by the IDFC, in the discharge of its compliance obligations, as an accountable institution in terms of FICA. These obligations regulate the way the IDFC manages money and property during their business dealings with clients and prospective clients.

The RMCP introduces the "risk-based approach" in terms of which the IDFC should understand each of its clients and identify, assess, and mitigate against money laundering (ML) and terrorist financing (TF) risks posed by the client to the IDFC. The Customer Due Diligence (CDD) procedures followed in respect of a given client must be tailored to and commensurate with that client's MLFT risk as assessed by the IDFC in terms of the RMCP.

This RMCP is legally binding on all employees, and any non-compliance will be regarded by the IDFC as serious misconduct and a dismissible offence.

6. ROLES AND RESPONSIBILITIES

6.1 Board and Senior Management's Roles and Responsibilities

The IDFC Board of Directors and Senior Management are responsible for ensuring that the IDFC maintains effective internal AML/CTF systems and controls. The IDFC Board of Directors and Senior Management must, as per the provisions of Section 42A of FICA, ensure compliance by the IDFC and its employees with the provisions of FICA and its RMCP. The IDFC Senior Management has appointed a Compliance Officer, to assist the IDFC in the above regard.

6.2 Compliance Function

The compliance function assists the Board of Directors and Senior Management in certifying that the obligations of compliance with FICA is met.

6.3 Compliance Officer's Roles and Responsibilities

The appointed Compliance Officer will undertake to perform the following functions:

6.3.1 Familiarise him/herself with the AML and CTF Laws;

6.3.2 Determine the compliance obligations of the IDFC and the compliance risk that the IDFC and its employees face;

6.3.3 Ascertain the current level of compliance by the IDFC and its employees with the compliance obligations;

6.3.4 Ensure that all employees are trained on FICA and anti- money laundering compliance requirements;

6.3.5 Ascertain any special compliance requirements for instance software and training programmes that may be required;

6.3.6 Draft or review the FICA Risk Management Compliance Programme (RMCP) and prepare a budget for the implementation of measures to ensure compliance;

6.3.7 Ensure compliance by all relevant employees;

6.3.8 Monitor level of compliance;

6.3.9 Assist employees that must report suspicious, unusual transactions and activities; and

6.3.10 Manage any requests for information from Financial Intelligence Centre (FIC) and other relevant authorities.

7. LEGAL STATUS AND REVIEW OF RMCP

7.1 The IDFC must review this RMCP as and when the need arises in terms of Section 42(2)(C) of the FIC Act or if there is a change in the circumstances of the IDFC that warrants a review of the RMCP in between 1-year intervals, the Compliance Officer may effect such amendments to the RMCP as is appropriate in light of the changed circumstances.

7.2 A copy of these rules will be made available to every employee of the IDFC involved in transactions with clients (Business Finance and Properties departments). Every employee involved in transactions with clients must familiarise himself or herself with the Risk Management Compliance Programme.

7.3 The IDFC must review this RMCP as and when the need arises in terms of Section 42(2)(C) of the FIC Act or if there is a change in the circumstances of the IDFC that warrants a review of the RMCP in between 1-year intervals, the Compliance Officer may effect such amendments to the RMCP as is appropriate in light of the changed circumstances.

8. MONEY LAUNDERING AND COUNTER TERRORISM FINANCING LEGISLATION

8.1 Prevention of Organised Crime Act No 121 (POCA)

Introduce measures to combat organised crime, money laundering, and criminal gang activities, and provides for the prohibition of money laundering, it also provides for an obligation to report certain information and recovery of proceeds of unlawful activities.

8.2 Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA)

Provides for measures to prevent, combat terrorist related activities and provides for an offence of terrorism and other offences associated or connected with terrorist activities. Provides the mechanism to comply with United Nations Security Council Resolution.

9. THE ADOPTION OF RISK BASED APPROACH TO THE BUSINESS

9.1 What is Money Laundering?

9.1.1 It is the moving of proceeds of crime such that same is no longer associated with the underlying criminal activities;

9.1.2 There are three (3) stages of money laundering: Placement, Layering, and Integration.

9.2 What does Terrorist Financing mean?

9.2.1 Solicitation, collection and providing funds and assets with the intention to be used to support terrorist acts, terrorist organisations, and individual terrorists.

9.3 Risk Assessment and Understanding of Risk

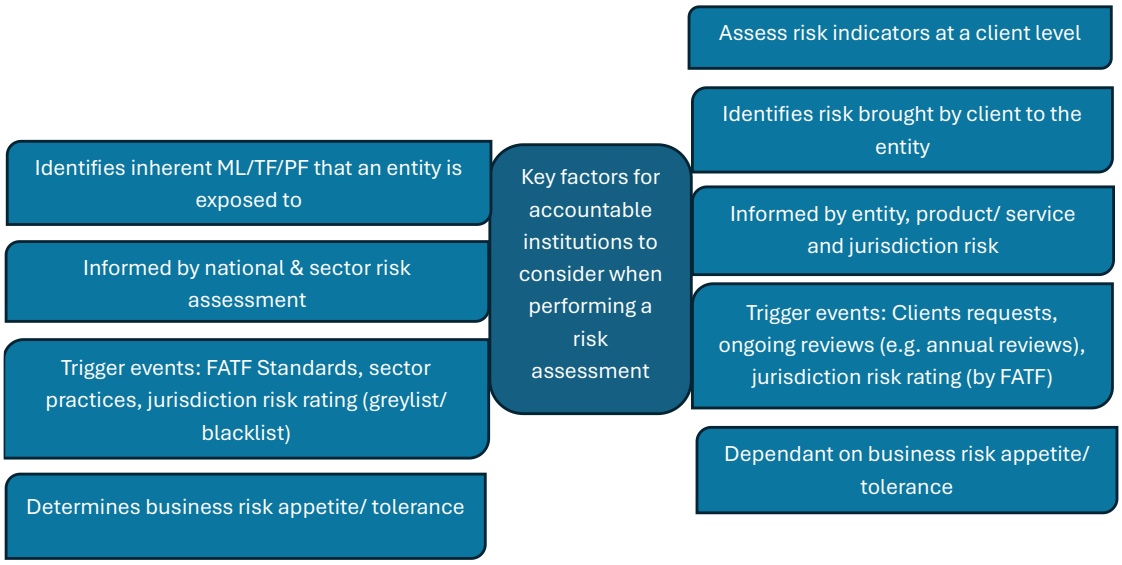
9.3.1 Risk Assessment

Identified risks are analysed to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact. A

range of results may be associated with a potential event, and management needs to consider them together.

This stage requires an intimate knowledge of the organisation, the market in which it operates, the legal, social, political, and cultural environment in which it exists as well as an understanding of strategic and operational objectives.

Entity-wide vs Client risk assessment



This is by far the most important step as the significance to each risk in the inventory is provided. This provides a tool for prioritising treatment efforts. The level of investments in controls would be indicated at this point.

The risk analysis herein assists the effectiveness and efficiency of the organisation by identifying those risks that require management attention.

Risk assessment allows consideration of the extent to which potential events might have an impact on achievement of objectives. It is about analysing and assigning ratings to the potential likelihood (frequency or probability) of an event occurring, and the potential consequence (impact or magnitude of effect), if the event does occur. The level of risk is determined by considering the combined effect of the likelihood and impact.

External and internal factors influence which events may occur and to what extent the events will affect the achievement of objectives. In risk assessment, management considers the mix of potential future events relevant to the organisation and its activities. There are three key principles for assessing risk:

- ensure that there is a clearly structured process in place;
- record the assessment of risk in a way which facilitates monitoring and the identification of risk priorities; and
- be clear about the difference between, inherent and residual risk.

Risk assessments should be expressed in the same unit of measure used for the key performance indicators for the organisation.

The residual risk should be benchmarked against the risk appetite for the organisation and management intervention applied if necessary.

This process must be conducted at least once a year or as often as necessary initiated by business requirements.

9.3.2 Inherent and Residual Risk

Inherent risk is the risk in the absence of any actions management might take or has taken to reduce either the risk's likelihood or impact. Should there be existing controls, these must not be considered when estimating the inherent risk value. Inherent risks are rated, assuming that there are no controls in place to mitigate the risk.

The existence of controls, depending on how adequate and effective they are based on assurance provider's assessment of all critical controls, may influence the likelihood or impact of the risk. This means that risk likelihood or impact may be reduced. Residual risk is the risk that remains after considering the effect of any existing controls.

Example: The risk of theft of a car may be rated high but having an immobilizer may reduce the likelihood of the risk occurring. The risk of theft may therefore be reduced.

In assessing risk, management considers the impact of expected and unexpected potential events. Many events are routine and recurring that have been addressed in management programmes and operating budgets. Others are unexpected, often having a low likelihood of occurrence but may have a significant potential impact. Unexpected events are responded on separately. However, uncertainty exists with respect to both expected and unexpected potential events, and each has the potential to affect strategy implementation and achievement of objectives. Accordingly, management assesses the risk of all potential events that are likely to have a significant impact on the achievement of objectives.

Risk assessment is applied first to inherent risks. Once risk controls and responses have been identified and/or developed, the residual risk is then determined.

9.3.3 Likelihood and Impact

Likelihood represents the probability that a given event or risk will occur while impact represents the effect of the risk should it occur.

Control

Management is responsible for designing, implementing, and monitoring the effective functioning of system of internal controls, but so is everyone in the institution consistent with their delegated authority. Controls are preventative, detective, or corrective and those would be management controls, administrative controls, accounting controls, and Information Technology controls. A control could be policies, procedures, laws, regulations, or any action that would reduce the likelihood or impact of a risk. For example: having an insurance policy or an alarm system will reduce the likelihood or impact of the risk of theft. Therefore, the insurance policy and alarm system are referred to as controls.

Step 1: Estimating likelihood and impact

Risk assessments are complex because the process involves subjective thinking. The identification of risks is based on an individual's experience and knowledge of the business and operations. Since experience and knowledge are unique to everyone, it is important to get a wide range of individuals on the risk management team. Each identified risk must be rated in terms of likelihood and impact.

Some types of risk lend themselves to a numerical diagnosis - particularly financial risk. For other risks - for example reputational risk - a much more subjective view is all that is possible. In this sense, a risk assessment is more of an art than a science. The assessment should draw as much as possible on unbiased independent evidence; consider the perspectives of the whole range of stakeholders affected by the risk.

Likelihood measures the probability that the identified risk / threat will occur within a specified period (between 1 and 3 years) on the basis that management have no specific / focused controls in place to address the risk / threat. The likelihood of occurrence must be assessed for every identified risk. Estimates of risk likelihood often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates. Internally generated data based on the institution’s own experience may reflect less subjective personal bias and provide better results than data from external sources. The ultimate likelihood agreed upon should be as realistic as possible based on all the known information at that point in time.

There are also more scientific and objective methods of determining the likelihood and impact of a risk.

The following rating scales have been established for the IDFC, i.e., Measures of likelihood of occurrence.

Measures of Likelihood Parameters

(a) Likelihood Parameters Table

Likelihood Factor	Qualification criteria	Rating
Almost certain	The risk is almost certain to occur in the current circumstances. The risk is already occurring or is likely to occur more than once within the next 12 months.	**5**
Likely	More than an even chance of occurring. The risk could easily occur and is likely to occur at least once within the next 12 months.	**4**
Possible	Could occur quite often. There is an above average chance that the risk will occur at least once in the next 3 years.	**3**
Unlikely	Small likelihood but could happen. The risk occurs infrequently and is unlikely to occur within the next 3 years.	**2**
Rare	Not expected to happen - Event would be a surprise. The risk is conceivable but is only likely to occur in extreme circumstances.	**1**

Measures of Impact (quantifying the impact of a specific risk occurring.)

(b) Measures of Impact Table

Impact Factor	Processes	People	Technical complexity	Financial
Catastrophic **5**	Major failure in internal processes resulting in substantial losses and errors.	Major losses to the value of the IDFC's collective competencies, knowledge, and skills. Serious breaches of the Code of Business Conduct and Ethics.	Use of unproven technology for critical system / project components. High level of technical interdependencies between system / project components.	> 15% of Revenue.
Critical **4**	Significant failure in internal processes resulting in high losses and errors.	Significant losses to the value of the IDFC's competencies, knowledge, and skills.	Use of new technology not previously utilised by the IDFC for critical systems / project components.	> 7.5% of Revenue.
Serious **3**	Moderate level internal processes impact.	Lower-level losses to the value of the IDFC's collective competencies, knowledge, and skills.	Use of unproven or emerging technology for critical systems / project components.	> 3.875% of Revenue
Significant **2**	Little internal processes impact.	Little impact to the value of the IDFC's collective competencies, knowledge, and skills.	Use of unproven or emerging technology for systems / project components.	> 2% of Revenue.
Insignificant **1**	No impact on internal processes.	No impact to the value of the IDFC's collective competencies, knowledge, and skills	Use of unproven or emerging technology for non-critical systems / project components	< 2% of Revenue

Step 2: Risk Matrix

Inherent risk exposure is the risk to the institution in the absence of any actions management might take to alter either the risk's impact or likelihood. Inherent risk is the product of the impact

of a risk and the probability of that risk occurring before the implementation of any direct controls. The score for inherent risk assists management and internal audit alike to establish relativity between all the risks / threats identified.

The ranking of risks in terms of inherent risk provides management with some perspective of priorities. This should assist in the allocation of capital and resources in the operations. Although the scales of quantification will produce an automated ranking of risks, management may choose to raise the profile of certain risks for other reasons.

The table below is to be used to assist management in quantifying the inherent risk of a particular risk (i.e., pre-controls).

Inherent Risk Exposure

(c) Inherent Risk Exposure Table

Category	Category description	Factor
Catastrophic	This risk should be terminated / insured / controlled	**≥ 25**
Critical	This risk should be insured / controlled	**21 –24**
Serious	This risk will typically be controlled (treated)	**16 – 20**
Significant	Management will make an informed decision as to whether this risk must be controlled or absorbed by the business unit. The decision will be based on a "cost vs. benefit" approach	**11 – 15**
Insignificant	Impact and probability is insignificant. This risk may be tolerated, and cost of losses will be absorbed by the operating unit	**1 – 10**

For example: A likelihood of 1 and impact of 5 would result in a risk index of 20 and this correlates to a low risk. In this way, each combination of likelihood and impact can be mapped to a risk index. The risk index indicates the severity of the risk.

Step 3: Determining the risk acceptance criteria by identifying what risks will not be tolerated

Risk appetite

Risk appetite is the amount of risk that is accepted in pursuit of achieving objectives. the IDFC has adopted a quantitative approach in determining risk appetite, reflecting, and balancing goals for growth, return, and risk. Risk appetite is related to strategy. It is considered in strategy setting, where the desired return from a strategy should be aligned with the risk appetite. Different strategies will expose different risks. Enterprise risk management, applied in strategy setting, helps management select a strategy consistent with risk appetite.

Defining a risk as acceptable does not imply that the risk is insignificant. The assessment should consider the degree of control over each risk; the cost impact, benefits and opportunities presented by the risk and the importance of the policy, project, function, or activity. Reasons for classifying a risk to be acceptable could include:

- the likelihood and impact of the risk could be so low that specific treatment is inappropriate;
- the risk being such that no treatment is available; and
- the cost of the treatment being so excessive compared to the benefit that acceptance is the only option.

The IDFC Risk Appetite Statement:

In pursuing the organisational objectives, no amount of risk is acceptable in any way by the organisation if it will lead to any kind of injury or death.

For all other identified risks both operational and strategic risks, wherein the residual risk rating is 16 (the product of impact and likelihood) and above up to 25, those risks need to be managed, and proof be made available. The Ithala Development Finance Corporation has no appetite for risks to the organisation in that specific range.

Step 4. Considering the Risk Response

Directed by the effectiveness of related internal controls

Management selects an approach or set of actions to align assessed risks with risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate responses to risks, including avoiding, accepting, reducing, and sharing risk.

Risk responses fall within the following categories the four T's of risk response:

- **Terminate** - Action is taken to exit the activities giving rise to risk. Risk terminate may involve exiting a project, avoiding high risk investments, or not accepting a pioneering technical solution.

- **Treat** - Action is taken to reduce the risk likelihood or impact, or both. This may involve any of a myriad of everyday business decisions.

- **Transfer** - Action is taken to reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common risk-sharing techniques include purchasing insurance products, pooling risks, engaging in hedging transactions, or outsourcing an activity, public private partnership. e.g., taking out forward cover for foreign currency purchases.

- **Tolerate** - No action is taken to reduce the likelihood or impact of a risk. e.g., not to factor earthquakes greater than 5 on the Richter Scale to bridge construction due to the rare/remote probability of any seismic activity in the geographical area.

Risk arising from Non-Compliance with Laws and Regulations

Non-Compliance with laws and regulations is not an option. All departments within the IDFC must understand the applicable legislation and must put in place controls to achieve compliance.

Where management of the risk is not within the control of the organisation, forward planning and lobbing should be considered, to ensure risk mitigation. For opportunities, the risk can be exploited, or reaction planning will include business continuity planning and disaster recovery planning.

The terminate response suggests that either the cost of other responses would exceed the desired benefit, or no response option was identified that would reduce the impact and likelihood to tolerate level. Treat and transfer responses reduce residual risk to a level that is in line within the risk appetites, while tolerate response suggests that inherent risk is already in line with risk appetites.

For many risks, appropriate response options are obvious and well accepted. For instance, a response option appropriate for the loss of computing availability is the development of a business continuity plan. For other risks, available options may not be readily apparent, requiring more extensive identification activities. For instance, response options relevant to mitigating the effect of global warming may require research on weather patterns and water availability.

In determining the appropriate responses, management should consider such things as:

- Evaluating the effectiveness of existing measures on treating the risk to tolerance level.
- Considering if there are other control measures that could be used to mitigate the risk more effectively. This is where benchmarks and leading practices are important. In the public sector, there are many opportunities to benchmark and consider leading practices as applied in other government institutions, provincial departments, or local authorities.
- Assessing the costs versus benefits of potential risk responses.

Step 5. Evaluating Effect of Response on Residual and Desired Residual Risk

Each risk is rated according to the inherent risk rating criteria. The effectiveness of the existing risk responses is assessed for these risks. This is done by rating the control effectiveness. A decision is then needed to determine if the risk is managed to the desired levels of risk appetite. This is an assessment of the current residual risk.

Controls are the management activities / policies / procedures / processes / functions / departments / physical controls that the institution and Management have put in place, and rely upon, to manage the strategic and significant risks. These actions may reduce the likelihood of occurrence of a potential risk, the impact of such a risk, or both. When selecting control activities management needs to consider how control activities are related to one another.

Management then needs to assess the control effectiveness based on their understanding of the control environment currently in place. At this stage of the process, the controls are un-audited and rated according to management's interpretation of control effectiveness.

The table below is to be used to assist management in quantifying the perceived and desired control effectiveness to mitigate or reduce the impact of specific risks.

The desired effectiveness of risk responses is determined where the desired risk exposure is not achieved with current risk responses. The desired effectiveness is measured on the same scale as the rating for current control effectiveness. This is the assessment of desired residual risk for each risk - sometimes referred to as risk tolerance. The sum of risk tolerances should measure risk appetite.

Residual risk is calculated by multiplying the inherent risk score [9.3.4 Inherent risk exposure Table] by the rating scale for control effectiveness.

(d) Control Effectiveness Table

Effectiveness Factor	Qualification criteria	Rating
Very High	Risk exposure is effectively controlled and managed.	**5**
High	Majority of risk exposure is effectively controlled and managed.	**4**
Medium	There is room for some improvement.	**3**
Low	Some of the risk exposure appears to be controlled, but there are major deficiencies.	**2**
Very low	Control measures are ineffective.	**1**

Residual Risk Exposure

The table below is to be used to categorise the residual risk exposure into the five different categories.

(e) Residual Risk Exposure Table

Category	Level	Category description	Factor
Priority 1	**Immediate action required**	Management should take immediate action to reduce residual risk exposure to an acceptable level.	**≥ 21**
Priority 2	**Action required**	Management should implement more controls or increase the effectiveness of current controls to reduce the residual risk to a more acceptable level.	**11 - 20**
Priority 3	**Monitor**	Management should constantly monitor the risk exposure and related control effectiveness.	**6 - 10**
Priority 4	**Acceptable**	The residual risk exposure is acceptable.	**2.6 - 5**
Priority 5	**Reduce control**	Management may consider reducing the cost of control.	**1 - 2.5**

9.4 Risk Based Approach to Customer Due Diligence

Risk based approach objectives are:

- To provide assurance that the IDFC has identified its risk exposures and has taken steps to properly manage them.
- To ensure that the IDFC's business planning processes focus on high-risk areas where risk management is required.
- To establish a process across the IDFC that will integrate the various risk control measures that are already in place.

The risk-based approach is classifying two phases in risk assessment process which is business Risk Assessment and Customer risk assessment.

9.4.1 Business Risk Assessment (as defined in the investment policies of the IDFC)

9.4.1.1 The IDFC is a Provincial development corporation based in KwaZulu-Natal (KZN). Its client has South African citizens, legal person, and foreigner with permanent residence in KZN.

9.4.1.2 A transaction is broadly defined in FICA as a transaction concluded between a client and an Accountable Institution (IDFC) in accordance with the type of business carried on by that institution and is not limited to transactions involving the flow of money and the following is a list of IDFC products:

Properties Department

- Large scale factories in Industrial estates
- Light industrial and SMME properties
- Commercial and retail properties
- Municipal Services (electricity, water and refuse removal)

Business Finance

- Micro-finance
- Working Capital Finance
- Agri-Finance
- Asset-based Finance
- Commercial Property Finance
- Procurement Finance
- Structured Finance
- Project Finance

9.4.2 Customer Risk Assessment

A customer of IDFC is regarded as a business legal entity or sole proprietor wishing to do business with IDFC in respect entering into a lease agreement for rental space or alternatively applying for a business loan. The IDFC must know the risk that is posed by each client and perform a client profiling assessment to identify the high risk and low risk client. The Customer Risk Assessment approach is not to seek to quantify the metrics used to measure risk. Rather,

a binary approach is adopted, which distinguishes between high risk, medium and low risk, doing so on a qualitative basis.

9.4.2.1 Who are high-risk clients?

9.4.2.1.1 Any natural person, legal person who is Domestic Politically Exposed Persons (DPEP);

9.4.2.1.2 Any natural person, legal person who is Foreign Politically Exposed Persons (FPEP);

9.4.2.1.3 Any natural person, but is not a citizen or permanent resident of South Africa;

9.4.2.1.4 A partnership, trust, company, or close corporation, regardless of whether it was formed in South Africa;

9.4.2.1.5 A person who is reluctant or refuses to provide information; or

9.4.2.1.6 An unusual or inexplicable preference for dealing with the Business via correspondence or via electronic media, as opposed to in person, particularly for the purposes of the CDD;

9.4.2.1.7 Deliberate evasiveness or vagueness when providing information;

9.4.2.1.8 Any other conduct or circumstances that, when viewed objectively, and when considered considering all the relevant factors taken as a whole, should be regarded with suspicion.

9.4.2.2 Who are the medium risk clients?

9.4.2.2.1 Any family member and/ known close associates of a person in a foreign or domestic prominent position.

9.4.2.3 Who are the low-risk clients?

9.4.2.3.1 Individuals or businesses whose single transaction or business relationship will be financed through a Cash payment of R5000 (five thousand rand) of business transaction.

9.4.2.3.2 The products and services that the business provides that are homogeneous or of a narrow range and not overly sophisticated; and

9.4.2.3.3 The business' transactions often involve two other Accountable Institutions, namely banks and conveyancing attorneys.

9.5 Risk Mitigation to ML/TF

9.5.1 The IDFC screens all the new clients and existing clients (Business Finance and Properties Department).

- **New Clients**: All new clients must be screened during the application stage.
- **Existing Clients**: All the existing clients must be screened through batch uploads; this is an ongoing process conducted on a quarterly basis to monitor and establish any defaults.

9.5.2 The IDFC uses systems and tools to screen the clients against the UN1267 Sanction list and FPEP, DPEP to mitigate the risk of ML/TF that may pose by their clients.

9.5.3 The IDFC has a policy in place to guide on how to deal with DPEP/FPEP. Clients who are identified as DPEP and FPEP will be dealt with in accordance with the IDFC DPEP and FPEP policy.

10. CUSTOMER DUE DILIGENCE (CDD) Section 20A-21H of the FIC Act

The customer due diligence refers to the knowledge that the IDFC has about its client and the business that the client is conducting (know your client).

10.1 Business Relationship

A business relationship in FICA is defined as “an arrangement between a client and the IDFC for the purpose of concluding transaction(s) on a regular basis.” The purpose of this RMCP is to provide clearly for the procedures, which must be followed by the IDFC in the discharge of its compliance obligations as an accountable institution in terms of FICA.

10.1.1 Establishing and Verification of Identities of a Natural Person and Residential Address

10.1.1.1 In respect of a natural person who is a citizen or resident of South Africa, identification can be determined by reference sources of information such as green bar-coded identity document or the new SA Smart card, passport issued by the Department of Home Affairs and driver’s licenses.

10.1.1.2 In cases of Foreign Nationals, the IDFC official should verify the identity by reference sources of information such as valid Passport, foreign identity documents, refugee permits, work permits and visitors visas of such individual with the relevant Authorities where possible.

10.1.1.3 This verification of the client’s identity is based on a view that the client is met face to face when his/her particulars are obtained and the IDFC does not deal with non-face to face clients.

10.1.1.4 The Representative of the IDFC must identify and verify the client’s identity as prescribed when a new transaction is entered into with an existing client unless the verification process was carried out within a 3 months’ period.

10.1.1.5 Residential addresses of natural persons must always be verified when entering a new transaction. Documents used to verify residential addresses must not be more than three months old, (except for the lease agreement, the current lease agreement is acceptable).

10.1.1.6 Documents that may offer confirmation of residential address include the following (list is not exhaustive):

- Utility bill reflecting name and residential address of the client.
- A bank statement from another bank reflecting the name and residential address of the client.
- Municipal rates and tax invoices reflecting the name and residential address of the client.
- Telephone or cell phone statement reflecting the name and residential address of the client.
- A valid (unexpired) lease or rental agreement reflecting the name and residential address of the client.
- Mortgage statement from another institution reflecting the name and residential address of the client.
- Valid television license reflecting the name and residential address of the client.
- Recent long-term or short-term insurance policy document issued by an insurance company and reflecting the name and residential address of the client.
- Recent motor vehicle license documentation reflecting the name and residential address of the client.

10.1.1.7 Copies of the documents must be in good condition (legible), be clear enough to be used for tracing or re-identification.

10.2 Establishing and Verification of Identities and Residential Address of Legal Person, Trust, and Partnership

In cases where an IDFC official is dealing with a Legal person, Trust, and Partnership (this is referred to as corporate vehicles) the residential address of the person acting or who purports to be authorized to establish a business transaction with the IDFC on behalf of the legal entity. The physical address of the business must be verified by the IDFC official. The additional due diligence is required to verify the identities of corporate vehicles. An IDFC official must carry out an addition due diligence investigation to establish:

i. the nature of the client business;
ii. the ownership and control structure of the business;
iii. the beneficial ownership of the business.

To establish and verify the identities of the beneficial owner of the legal person. (Refer to **Annexure A**)

10.3 Anonymous OR Fictitious Clients

10.3.1 The IDFC is prohibited from dealing with anonymous persons, or persons who have fictitious names, and the IDFC does not deal with non-face to face clients.

10.3.2 The IDFC must, abide by to the requirements of the act to ward against the risk of:

- Dealing with an anonymous person by refusing to on-board as a client anybody who appears to desire or expresses a desire to transact with the IDFC anonymously.
- Dealing with a fictitiously named person by subjecting all prospective clients to the CDD procedures, which are intended at ensuring, amongst other things, that the business only deals with persons who exist.

10.4 On-going due diligence measure relating to legal person, trust, and partnership.

10.4.1 Section 21C of the FICA provides for ongoing due diligence measures. These measures follow the obligation to understand the purpose and intended nature of a business relationship.

10.4.2 The IDFC Compliance Function monitors client statements and accounts against the information provided by the client in the questionnaire pertaining to the:

- nature of the Business Relationship;
- the purpose of the Business Relationship;
- the source of the funds that will finance the Business Relationship; and
- must update such information and any other documents originally forming part of the CDD in respect of that Client where necessary.

10.4.3 The IDFC perform site inspection visits annually to ensure that the activities that are conducted in the premises are as per our knowledge of the client.

10.5 Section 21D Doubts About the Accuracy of Existing Information

10.5.1 Where IDFC has doubts about information that it previously obtained from an existing Client, it must take reasonable steps to satisfy itself as to that information's accuracy or otherwise, and such reasonable steps may include:

- requesting from the Client an original document if a certified copy thereof was originally accepted; or
- requesting from the Client a copy that is certified more recently than the copy that was originally accepted; or
- requesting from the Client a document generated by a Governmental Authority or other independent person, where a document generated by the Client was originally accepted.

10.6 Inability to conduct customer due diligence.

10.6.1 The IDFC must terminate a Business Relationship with a Client in respect of whom a CDD or ongoing CDD cannot be conducted.

10.6.2 An employee who is unable to conduct the CDD or ongoing CDD must, immediately upon realising his or her inability, inform the Risk Officer in writing thereof.

10.7 Section 21F and 21 G of FICA PEP & PIP Customer due diligence

10.7.1 Source of funds vs source of wealth

10.7.2 The FIC Act requires accountable institutions to establish source of funds and source of wealth throughout the course of a business relationship.

10.7.3 **Source of funds:** The origin of the funds upon the commencement of a business relationship/transaction.

10.7.3.1 Salary

10.7.3.2 Lottery or gambling winnings

10.7.3.3 Sale of property

10.7.3.4 Inheritance

10.7.4 **Source of wealth:** Activities that have generated the total net worth of the client that is, the activities that produced the client's funds and property. This can include:

10.7.4.1 Past earnings

10.7.4.2 Investments

10.7.4.3 Inheritance

10.7.4.4 Any business dealings that have contributed to their current wealth

10.8 Based on the outcome of the CDD, it may be necessary to undertake an Enhanced Customer Due Diligence (EDD), as outlined under section 11 below.

11. ENHANCED DUE DILIGENCE (EDD)

Institutions are required to undertake an Enhanced Due Diligence (EDD) process, in respect of clients who are categorised as higher risk. Higher risk clients are defined under 9.4.2.1. Higher risk clients and clients with larger transactions pose greater risks to the organisation, therefore, close monitoring is required. For clients defined under 9.4.2.1, an EDD must be undertaken according to the following guidelines:

11.2.1 Detailed documentation relating to the business transaction and the client must be obtained and scrutinised. Such information may include but is not limited to:

11.2.1.1 Identity information, address information of the individuals and business entities;
11.2.1.2 Performing a comparison of the nature of the business versus the transaction at hand and whether there is correlation between the two;
11.2.1.3 Performing a comparison between the turnover recorded on the financial statements and those received through the Bank account would reveal that there is a possibility of transactions being concluded on a cash basis, and should there be such a discrepancy, there is a need to request for invoices to account for the discrepancy;

11.2.1.4 Identifying clients who prefer dealing through electronic means and not face to face, in this instance IDFC must enforce a face-to-face meeting and site visit;
11.2.1.5 Pay special attention to the countries in which the client does business with (Grey listed countries), and where such situations arise, these should be escalated to higher management for a decision as to whether to proceed with the transaction or not;
11.2.1.6 Identify businesses which present a higher risk of money laundering, whereby the nature of the business does not match the turnover being presented. In this instance, IDFC must ensure that there is an adequate due diligence performed on the financial statements, which may require that the IDFC official requests audited financial statements.
11.2.1.7 In respect of properties leased by IDFC, Properties department must identify the source of rental payments on the rental account, and whether these are in line with the agreed lease payments. In an instance where the payment is vastly higher, the source of these funds must be queried with the client and reported as a suspicious transaction to the FIC, should the client not be able to provide a plausible response or in instances where the client requests a partial refund against the account shortly after payment, this may represent a money laundering risk.

21A. Understanding and obtaining information on business relationship.

When an accountable institution engages with a prospective client to establish a business relationship as contemplated in section 21, the institution must, in addition to the steps required under section 21 and in accordance with its Risk Management and Compliance Programme, obtain information to reasonably enable the accountable institution to determine whether future transactions that will be performed in the course of the business relationship concerned are consistent with the institution's knowledge of that prospective client, including information describing–
(a) the nature of the business relationship concerned;
(b) the intended purpose of the business relationship concerned; and
(c) the source of the funds which that prospective client expects to use in concluding transactions during the business relationship concerned.

21B. Additional due diligence measures relating to legal persons, trusts, and partnerships.

(1) If a client contemplated in section 21 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 the steps required under sections 21 and 21A and in accordance with its Risk Management and Compliance Programme, establish–
(a) the nature of the client's business; and
(b) the ownership and control structure of the client.
(2) If a client contemplated in section 21 is a legal person, an accountable institution must, in addition to the steps required under sections 21 and 21A and in accordance with its Risk Management and Compliance Programme–
(a) establish the identity of the beneficial owner of the client by–
(i) determining the identity of each natural person who, independently or together with another person, has a controlling ownership interest in the legal person;

(ii) if in doubt whether a natural person contemplated in subparagraph (i) is the beneficial owner of the legal person or no natural person has a controlling ownership interest in the legal person, determining the identity of each natural person who exercises control of that legal person through other means, including through his or her ownership or control of other legal persons, partnerships or trusts; or
(iii) if a natural person is not identified as contemplated in subparagraph (ii), determining 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; and
(b) take reasonable steps to verify the identity of the beneficial owner of the client, so that the accountable institution is satisfied that it knows who the beneficial owner is.

21H. Family members and known close associates.

(1) Sections 21F and 21G apply to immediate family members and known close associates of a foreign or domestic politically exposed person or a prominent influential person.
(2) For the purposes of subsection (1), an immediate family member includes–
(a) the spouse, civil partner, or life partner;
(b) the previous spouse, civil partner, or life partner, if applicable;
(c) children and stepchildren and their spouse, civil partner, or life partner;
(d) parents; and
(e) sibling and step sibling and their spouse, civil partner, or life partner.

7A Amendments: Immediate family member

- Known close associate.
- Examples of known close associates extracted from guidance provided by the FATF include the following types of relationships:
- Known sexual partners outside the family unit such as girlfriends, boyfriends, extra-marital partners.

DPEPs: Domestic Politically Exposed Person (DPEP) and Foreign Politically Exposed Person (FPEP)

When dealing with a foreign politically exposed person, a high-risk domestic politically exposed person and/or immediate family members or known close associates of these persons, an accountable institution must:

- Obtain senior management approval to establish a business relationship;
- Establish their source of wealth; and
- Conduct enhanced due diligence.

Geographic Area Risk Assessment

When assessing the risk posed by geographic area consider:

- Is the client domiciled in South Africa or in another country, or does the client operate in another country?
- Do clients who are domiciled or operating outside South Africa engage with the institution in South Africa or through branches, subsidiaries, or intermediaries outside South Africa?

- Have credible sources identified geographic locations from where clients engage with an institution as high-risk jurisdictions?
- Are the geographic locations from which clients engage with an institution subject to sanctions regimes?
- Is the client a foreign politically exposed person from a high-risk jurisdiction, or considered to have high risk of corruption?
- If the client is a corporate vehicle, has it been incorporated in a country which has been identified by credible sources as a high-risk jurisdiction or in a country which is the subject of a sanction's regime, or does it operate in such a country?
- Has an international body, a domestic regulator or supervisory body or other credible source expressed concern about weak regulatory measures against Money Laundering and Terrorist Financing, weak transparency requirements for beneficial ownership of corporate structures or weak institutional frameworks such as supervisory, law enforcement and prosecuting agencies in relation to a geographic location from where clients engage with an institution?
- Are the geographic locations from where clients engage with an institution known to applying excessive client confidentiality?

12. FOREIGN POLITICALLY EXPOSED PERSONS (FPEP) AND DOMESTIC POLITICALLY EXPOSED PERSONS (DPEP)

FPEP and DPEP are the terms used for an individual who is or has in the past been entrusted with prominent public functions in a particular country (this section must also be read in conjunction with the Domestic Politically Exposed Persons (DPEP), Foreign Politically Exposed Persons (FPEP), and Prominent Influential Persons (PIP) policy. This list serves as an example of who could be regarded as FPEP and DPEP:

12.1 LIST OF FPEP POSITIONS

The following positions in respect of countries other than South Africa are FPEP positions:

- Head of State;
- Member of royal family;
- Member of cabinet or similar structure;
- Senior member or leader of a political party;
- Senior judicial officer;
- Senior executive of a state-owned entity; or
- High-ranking military officer.

12.2 LIST OF DPEP POSITIONS

The following people are DPEPs:

- President or deputy president of South Africa;
- Cabinet Minister or Deputy Minister;
- Premier of a province;
- Member of Executive Council of a Province;

- Mayor of a municipality;
- Leader of a political party;
- Member of a royal family or a senior traditional leader;
- Head, accounting officer or chief financial officer of a national or provincial department;
- Manager or chief financial officer of a municipality;
- Chairperson, chief executive officer, accounting authority, chief financial officer, or chief investment officer of a public entity;
- Prominent judge in the Constitutional Court, Supreme Court of Appeal, or the High Court or any equivalent court;
- Ambassador, high commissioner, or senior representative of a foreign country who is based in South Africa.

13. REPORTING SUSPICIOUS, UNUSUAL TRANSACTIONS AND CASH THRESHOLD

13.1 Cash Threshold Reporting (CTR)

13.1.1 All Accountable and Reporting Institutions must report all cash transactions exceeding R49 999.99 to FIC. This refers to any transactions where the cash threshold can be a single transaction to the value of R49 999.99 or an aggregation of small amounts with a combined value of R94 999.99 or more. A period of 72 hours must be applied when considering aggregate.

13.1.2 Indicators of when a series of small accounts combine to form a composite transaction that exceed the prescribed threshold are as follows:

13.1.2.1 The period within which such small a series of smaller transactions take place.

13.1.2.2 The fact that the series of transactions consist of a repetition of the same type of transaction e.g., cash payments or cash deposits.

13.1.2.3 The smaller amount transactions involve the same person or account holder or relates to the same account.

13.1.2.4 The IDFC Money Laundering and Reporting Officer (MLRO) must monitor these transactions daily by downloading the IDFC bank account statements, analyze them for transactions of R49 999 or more and report all the reportable transactions (including aggregated transactions) through the Orbital Solution System that interfaces with the FIC goAML system within the pre-scribed period (two business days) of the transaction. All transactions that have been reported are then cross-referenced to ensure successful submission to the Financial Intelligence Centre (FIC).

13.2 Suspicious and Unusual Transactions (STR)

Suspicious and Unusual transactions are transactions that you have reasonable grounds to suspect are related to the commission of a money laundering offence, suspicious transactions also include financial transactions that you have reasonable grounds to suspect are related to the financing of terrorists.

13.3 Indicators of Suspicious and Unusual Transactions

13.3.1 The following are a few indicators of suspicious and unusual transactions:

13.3.1.1 Any transaction that is unusually larger, otherwise inconsistent with the customer's financial standing or usual pattern of activities.
13.3.1.2 A client attempts to convince an employee not to complete any documentation required for the transaction.
13.3.1.3 A client has unusual knowledge of the law in relation to suspicious transaction reporting.
13.3.1.4 A client seems very conversant with money laundering or terrorist activity financing issues.
13.3.1.5 A client is quick to volunteer that funds are clean or not being laundered.
13.3.1.6 A client provides doubtful or vague identification information.
13.3.1.7 A client refuses to produce personal identification documents.
13.3.1.8 A client changes a transaction after learning that he must provide a form of identification.
13.3.1.9 A client only submits copies of personal identification documents.
13.3.1.10 A client's supporting documentation lacks such as contact particulars.
13.3.1.11 A small business in one location makes deposits on the same day at different branches.
13.3.1.12 Accounts that show unexpectedly large cash deposits.
13.3.1.13 Involvement of significant amounts of cash in circumstances that are difficult to explain.

13.4 Triggers for Reporting

13.4.1 The duty to report is triggered where any employee knows or suspects that the IDFC is party to a transaction that:

13.4.1.1 Has received proceeds of unlawful activity or it is about to receive such proceeds.
13.4.1.2 Has received property which is connected to an offence relating to the financing of terrorists' activities, or it is about to receive such property.
13.4.1.3 Has been used in some way for money laundering purposes or it is about to be used for same.
13.4.1.4 Has been used in some way to facilitate an offence relating to the financing of terrorist activities.

13.5 Reporting

13.5.1 The duty to report overrides any duty of confidentiality owed by the IDFC to the client. On receipt of the suspicious report, the Compliance Officer must be briefed on FICA related matters.

13.5.2 The person forming the suspicion must draft an email (also attach relevant documents) setting out the basis of the suspicion and submit it to the Compliance Officer and/or MLRO.

13.5.3 The Compliance Officer will investigate the matter and decide whether a report must be made to the FIC. In coming to that decision, the Compliance Officer will consider the profile of the client and discuss the matter, with the person reporting the suspicion, as well as the Head of Department.

13.5.4 The Compliance Officer must report to the FIC as soon as possible but not later than 15 days excluding Saturdays, Sundays, and public holidays after becoming aware of such STR. The

particulars to be reported and the manner of reporting are contained in Regulation 22 and Regulation 23 of FICA, respectively.

13.5.5 Any person who is employed by the IDFC may report suspicious and unusual transactions relating to unlawful proceeds connected to the affairs of the IDFC under exceptional circumstances.

13.5.6 The Compliance Officer must maintain a register of reports submitted to the FIC.

13.5.7 Once the matter has been reported to the FIC, the person who made the report must be informed that under no circumstances must the fact that the matter has been reported or may be reported be communicated to the client. To do so would constitute "tipping-off" and this is an offence under FICA.

13.5.8 A person who has reported as set out above will have discharged his or her obligation to report in terms of FICA. This obligation is discharged whether the Compliance Officer reports the suspicion to the FIC.

13.5.9 A person may continue with the transaction. Unless of course, the FIC directs that the transaction should not be proceeded with, effect must be given to this direction or instruction forthwith.

13.5.10 A further reason for requiring all suspicions to be reported to the Compliance Officer is that the receipt of these reports will enable the IDFC to build a database and will be used in training relating to suspicious transactions.

13.6 Property Associated with Terrorists

13.6.1 Properties Department should ensure that the leased property is leased for the correct and lawful purpose in order to avoid accommodating terrorist's activities in our properties by having Key Controls and procedures in place to deal with this aspect as well as by verifying the personal details of our prospective clients, all clients must be screened using World-Check one (both entity and individual directors/members must be screened).

13.6.2 If the IDFC has any property, which is connected to any terrorist activities, the Compliance Officer must be informed immediately, and the report must be filed with the FIC in terms of section 28A as soon as possible.

13.7 Protection of Person Making Report

13.7.1 No action, whether criminal or civil, lies against any person complying in good faith with the reporting obligations under FICA.

13.8 Suspicious Activity Report (SAR)

13.8.1 'SAR' refers to a suspicious or unusual activity report submitted to the FIC in terms of section 29 (1) (a) or (c), the IDFC uses Orbital Middleware Reporting to report suspicious and unusual activities to the FIC.

13.8.2 The following options are selected when reporting:

13.8.2.1 Capture new SAR, suspicious details, action taken, involved activities, save and commit report.

13.8.2.2 A person who has made, initiated or contributed to a report in terms of FICA or who has furnished additional information concerning such a report is competent, but not compellable, to give evidence in criminal proceedings arising from the report.

13.8.2.3 No evidence concerning the identity of a person who has made, initiated or contributed to such a report or who has furnished additional information concerning such a report is admissible as evidence in criminal proceedings unless that person voluntarily testifies at those proceedings.

13.9 Targeted Financial Sanctions

13.9.1 Implementation of the United Nations Security Council (UNSC) resolutions relating to the freezing of assets.

13.9.1.1 South Africa's Targeted Financial Sanctions (TFS) obligations require accountable institutions to scrutinise information concerning clients against TFS lists, apply freezing of assets of designated persons or entities, and file terrorist property regulatory reports with the Centre.

13.9.1.2 No person may directly, indirectly, in whole or in part enter into or facilitate a transaction for persons or entities listed on the UNSC resolutions.

13.9.1.3 This prohibition in section 26B of the FIC Act is applicable, but not limited to, all instances where the designated person or entity is:

- The client;
- The person acting on behalf of the client;
- The client acting on behalf of another person;
- A beneficial owner of the client; and
- A party to a client's transaction, including a party who benefits in any way from a client's transaction.

14. DIRECTIVE 8- SCREENING OF EMPLOYEES FOR COMPETENCY AND INTEGRITY

14.1 In terms of **Directive 8** issued by the FIC and gazetted on 31 March 2023, accountable institutions are required to have adequate processes and controls in place to:

14.1.1 Ensure screening of prospective and current employees for competence and integrity, using a risk-based approach.

14.1.2 Scrutinise prospective and current employee information against the targeted financial sanction lists, to mitigate and manage the risk of money laundering, terrorist financing, and proliferation financing.

14.2 ***Prospective employees***-in adopting Directive 8, the following screening processes currently apply to the IDFC as part of risk mitigation, prior to an appointment being made:

14.2.1 Criminal checks conducted for all employees (including interns and contract workers);

14.2.2 State Security screening undertaken for Executive positions and Board members;

14.2.3 Credit Bureau checks;

14.2.4 Qualification verification;
14.2.5 Accreditation verification;
14.2.6 Reference checks in respect of previous employment, experience, and integrity;
14.2.7 Terrorist Finance and money laundering checks against the FIC online list for all new employees, irrespective of level;
14.2.8 Panel and structured interviews conducted and documented, to ensure that the potential incumbent possesses the necessary skills, knowledge, and expertise to perform the function effectively.
14.2.9 New employees' complete declarations of interest.

14.3 ***Current employees***- in adopting Directive 8, the following ongoing risk mitigation measures apply:

14.3.1 Terrorist Finance and money laundering check against the FIC online list for all current employees, irrespective of level conducted on an **annual** basis;
14.3.2 Annual declarations of interest completed by all employees;
14.3.3 In dealing with client and business-related matters, declaration of any conflict is undertaken at all committee meetings and documented;
14.3.4 Ongoing Ethics awareness and training workshops conducted in promoting an ethical culture within the organisation.
14.3.5 Anti-Fraud and Ethics policy, together with the Whistleblowing policy and Ethics Management strategy are brought to the attention of existing employees periodically, to promote sound and ethical behaviour.

14.4 In dealing with any adverse outcomes that may arise out of the screening process, such results are to be referred to the Line Manager, Departmental Executive, Group Chief Risk Officer, Corporate Services Executive and the Group Chief Executive for deliberation and a way forward which must be addressed in accordance with the LRA.

14.5 The required screening under Directive 8 of FIC includes members of Boards of accountable institutions and will therefore include Board members of the IDFC board and boards of subsidiary entities.

14.6 All employee integrity and competency screening information are retained in employee files. Terrorist Finance and money laundering checks against the FIC online list for all new and current employees are stored electronically.

15. RECORD KEEPING

15.1 In terms of FICA the IDFC is required to keep detailed records of its clients and the transactions entered with them.

15.2 The duty to keep records arises whenever the IDFC establishes a business relationship or concludes a single transaction with a client.

15.2.1 FICA obliges the IDFC to keep records of the following:

15.2.1.1 The Identity Document of a client.
15.2.1.2 Proof of residential address.
15.2.1.3 Proof of registration of the Company in case of a Company.

15.2.1.4 The nature of the business relationship or transaction.

15.2.1.5 In the case of transaction, the amount involved and the parties to that transaction.

15.2.1.6 All accounts that are involved in transactions concluded by the IDFC during a business relationship or a single transaction.

15.2.1.7 The name of the person who obtained the information referred to above; and

15.2.1.8 Any document or copy of a document obtained by the IDFC to verify a person's identity.

15.3 Procedure for Record Keeping

15.3.1 The divisional managers from the Properties and Business Finance Departments, must appoint a responsible employee to ensure that record keeping processes are established and maintained.

15.3.2 Client files (Hard copies) should be kept in a secure and fireproof safe storeroom.

15.3.3 Access to such safe storeroom shall be restricted to the responsible employee who has been appointed.

15.3.4 The responsible employee must create a file register, to record the movement of client files from the storeroom.

15.3.5 Files should not be kept in the office cabinets of the IDFC employees or managers.

15.3.6 Each client should have a folder for FICA documents in terms of the Document Management System. Hard copies of records should also be scanned and kept electronically.

15.3.7 Copies of electronic records will be kept by Metro file and regular back-ups of electronic records will be made and stored securely. Identification and verification documents stored off-site will be retrievable within 5 working days.

15.3.8 This procedure is applicable to all the IDFC business units which are affected by the FIC Act.

15.3.9 Records must be kept for a period of five years from the date on which the business relationship is terminated. Business units should have procedures which deal with this aspect. Such Key Controls should be in line with these RMCP.

15.3.10 No person may delete or destroy any record pertaining to a client in respect of identity or verification of identity or in respect of any transaction recorded.

15.3.11 An authorized representative of the FIC has access to any records kept by the IDFC in terms of FICA and may examine, make extracts from or copies of any such records.

15.3.12 The IDFC must, except of course where such documents are protected by legal professional privilege, give to an authorized representative of the FIC all reasonable assistance in this regard.

15.3.13 Any request for access to records, must be forwarded to the Compliance Officer or the assistant Compliance Officer and may not be dealt with by any member of staff.

16. FICA TRAINING

16.1 Training should be provided to all (new and existing) employees concerned on an on-going basis to enable them to understand the implications of non-compliance with FICA.

16.2 All new employees will attend a training session during their induction program.

16.3 New employees whose daily duties requires them to interact with clients should also receive FICA training within three to six months of joining the IDFC.

16.4 Considering the prevailing economic climate, the IDFC will endeavour to train and provide refresher training to its employees as and when the need arises.

17. FAILURE TO COMPLY WITH THIS RMCP

17.1 Failure to comply with this RMCP by any employee of the IDFC will constitute misconduct on behalf of the employee. Such employee will in addition to the sanctions imposed by FICA be subjected to the IDFC disciplinary code of conduct.

18. OFFENCES AND PENALTIES

18.1 In terms of new FIC Amendment Act, the FIC can either impose administrative sanctions or criminal sanctions in the following manner for non-compliance with the Act.

18.1.1 Potential fine/penalty of R10M.

18.1.2 Criminal penalty of 5 years' imprisonment (natural person) and a fine of R10M (entity).

18.1.3 Administrative penalty is R10M (natural person) and R50M (entity).

18.1.4 The IDFC may also be expected to pay the cost of the inspection.

ANNEXURE A

CLIENT IDENTIFICATION AND VERIFICATION LIST

Business Finance

TYPE OF ENTITY	DOCUMENTS	REPRESENTATIVES
Individual	• Certified copy of SA green bar-coded ID or new SA ID card. • Valid passports for foreign nationals • Proof of Residential Address (not older than 3 months • Any SARS document (with individual name and SARS number)	
Partnerships	• Partnership agreement • Any SARS document (with entity name and SARS number) • Proof of Business Address	• Certified copy of SA green bar-coded ID or new SA ID card or Legal identity documents of: each partner • Valid passports for foreign nationals • Proof of Residential/Business Address (not older than 3 months) of: each partner
Close Corporation	• Founding statement CK 1, or • Change of name (CK2) if applicable • Any SARS document (with entity name and SARS number)	• Certified copy of SA green bar-coded ID or new SA ID card or Legal identity documents of: each member • Valid passports for foreign nationals • Proof of Residential/Business Address (not older than 3 months) of: each member
Companies	• Notice of Incorporation (COR 14.1) • Registration Certificate (14.3) • Memorandum of Incorporation (15.1A) • Shareholders Certificate • Any SARS document (with entity name and SARS number) • Proof of Business Address	• Certified copy of SA green bar-coded ID or new SA ID card or Legal identity documents of: - each shareholder (who owns at least 25% of the Company's shares); - the person authorised to transact on behalf of the company and - Managing Director/CEO of the Company • Valid passports for foreign nationals • Proof of Residential Address (not older than 3 months) of: - each shareholder (who owns at least 25% of the Company's shares); - the person authorised to transact on behalf of the company and - Managing Director/CEO of the Company
Trust	• Trust Deed • Letter of Authority • Any SARS document (with entity name and SARS number) • Proof of Business Address	• Certified copy of SA green bar-coded ID or new SA ID card or Legal identity documents of - each trustee; - the person authorised to transact on behalf of the trust. - the executor / founder of the trust. • Valid passports for foreign nationals • Proof of Residential Address (not older than 3 months) of: - each trustee; - the person authorised to transact on behalf of the Trust and - the executor / founder of the trust.

TYPE OF ENTITY	DOCUMENTS	REPRESENTATIVES
Cooperatives	• Certificate of Incorporation / Registration (CR10) • Certificate Disclosure • Any SARS document (with entity name and SARS number) • Proof of Business Address	• Certified copy of SA green bar-coded ID or new SA ID card or Legal identity documents of: - For all Members/Directors; - the person authorised to transact on behalf of the cooperatives. • Valid passports for foreign nationals; • Proof of Residential Address (not older than 3 months) of: - For all Members/Directors; - the person authorised to transact on behalf of the cooperatives.

Properties

TYPE OF ENTITY	LEGAL DOCUMENTS	REPRESENTATIVES
Individual	• Certified copy of SA green bar-coded ID or new SA ID card. • Valid passports for foreign nationals • Proof of Residential Address (not older than 3 months • Any SARS document (with individual name and SARS number) *NB: For SMME tenants, SARS documents are not compulsory as a significant majority of these tenants are below the tax threshold for tax registering purposes.*	• Certified copy of SA green bar-coded ID or new SA SMART ID card. *(See note 1)* • Valid passports for foreign nationals • Proof of Residential Address (not older than 3 months).
Partnerships	• Partnership agreement • Copy of power of attorney, if more than one partner • Any SARS document (with entity name and SARS number)	• Certified copy of SA green bar-coded ID or new SA SMART ID card of: - each partner (who owns at least 25% of the partnership shares) *and* - of the person authorised to sign the lease (proxy). *(See note 1)* • Valid passports for foreign nationals • Proof of Residential Address (not older than 3 months) of: - each partner who owns at least 25% of the partnership shares; and - the person authorised to sign the lease (proxy).
Close Corporation	• Founding statement CK 1, or • Change of name (CK2) if applicable • Copy of Power of Attorney, authorising representative to sign the lease • Any SARS document (with entity name and SARS number)	• Certified copy of SA green bar-coded ID or new SA SMART ID card of: - each member (who owns at least 25% of the Close Corporation's shares); - person authorised to sign the lease (proxy); - the CEO / MD of the Close Corporation *(See note 1)* • Valid passports for foreign nationals • Proof of Residential Address (not older than 3 months) of: - each member who owns at least 25% of the close corporation's shares; - the person authorised to sign the lease (proxy) and - the CEO / MD of the Close Corporation.

TYPE OF ENTITY	LEGAL DOCUMENTS	REPRESENTATIVES
Companies *(Private Companies and unlisted public companies)*	• Notice of Incorporation (COR 14.1) • Registration Certificate (14.3) • Memorandum of Incorporation (15.1A) • Shareholders Certificate • Copy of Power of Attorney, authorising representative to sign the lease • Any SARS document (with entity name and SARS number)	• Certified copy of SA green bar-coded ID or new SA SMART ID card of: - each shareholder (who owns at least 25% of the Company's shares); - the person authorised to sign the lease (proxy) and - the CEO / MD of the Close Corporation *(See note 1)* • Valid passports for foreign nationals Proof of Residential Address (not older than 3 months) of: - each shareholder who owns at least 25% of the company's shares*;* - the person authorised to sign the lease (proxy) and - the CEO / MD of the company. *NB: JSE listed Companies are exempted from providing FICA docs.*
Trust	• Trust Deed • Letter of Authority • Resolution nominating trustee to enter a lease on behalf of the trust. • Any SARS document (with entity name and SARS number)	• Certified copy of SA green bar-coded ID or new SA SMART ID card of: - each trustee; - the person authorised to sign the lease (proxy); and - the executor / founder of the trust *(See note 1)* • Valid passports for foreign nationals • Proof of Residential Address (not older than 3 months) of: - each trustee; - the person authorised to sign the lease (proxy) and - the executor / founder of the trust.
Cooperatives / NGOs / Clubs / Associations / Political Parties / Trade Unions.	• Certificate of Incorporation / Registration / Constitution. • Letter of authority for the person signing the lease • Any SARS document (with entity name and SARS number)	• Certified copy of SA green bar-coded ID or new SA SMART ID card of each: - member (who owns at least 25% of the Entity's shares) *and* - of person authorised to sign the lease (proxy) *(See note 1)* • Valid passports for foreign nationals • Proof of Residential Address (not older than 3 months) of: - each member who owns at least 25% of the company's shares *and;* - of person authorised to sign the lease (proxy).

Note 1: If SA identification document cannot be provided, then valid SA Passport or driver's license may be accepted.

Note 2: If tenant cannot produce proof of address, then letter of confirmation (on proper letterhead) from local ward counsellor is acceptable, provided it is less than 3 months old.