Exim Bank Djibouti

Financial Crime Prevention Policy and AML Policy

VERSION CONTROL NUMBER	DATE	AMENDMENT NUMBER
5	July 2021	5/2021

Table of Contents

CONFIDENTIALITY

Any employee, (both past and present) contravening the above will be responsible for disciplinary action as per bank procedure

Preamble

This document sets forth the policy to be followed by Exim Bank Group ('the Bank') in preventing and deterring corruption, fraud, collusion, coercion, obstruction, money laundering and terrorist financing (jointly "*Financial Crime*") in the Bank's activities.

The Bank shall ensure that all of its activities, including, but not limited to, corporate and retail lending, mortgages, treasury activities, card services, etc., serve the intended purposes. In this context, the Bank shall endeavour to ensure that its activities are free from financial crime. The Bank shall work to prevent and deter financial crime from occurring and, where it does occur, will address it in a timely and expeditious manner. To this end, deterrence, prevention and investigation procedures shall also be adopted.

1. Source

- Law n°196/AN/02/4th L of 29 December 2002 on Money Laundering, Confiscation and International Cooperation in relation to the proceeds of crime, completed by law n°112/AN/6th L of 25 May 2011;

- Law n°110/AN/11/6ème L of 25 May 2011 on the repression of the financing of terrorism;
- Law n°111/AN/11/6ème L of 25 May 2011 on the fight against terrorism and other serious crimes;
- Decree No. 2006-0083/PR/MJAPM of 27 March 2006 implementing Law No. 196/AN/02/4th L of 29 December 2002 on Money Laundering, Confiscation and International Cooperation in respect of the Proceeds of Crime and on the organization and operation of the Financial Intelligence Unit;
- Law N° 03/AN/13/7th L supplementing the legislative provisions relating to the prevention and fight against corruption;
- The 40 recommendations on the fight against money laundering and terrorist financing, federated by the FATF (Financial Action Task Force)
- Standard decreed by the basses committe on customer due diligence
- EXIM's Group Anti-Money Laundering and Anti-Terrorist Financing Policy

- Instruction 203-01 on the Prevention and Combating of Money Laundering and the Financing of Terrorism

2. Introduction

This Financial Crimes Prevention policy (FC Policy) is established to facilitate the development and management of controls that will aid in the detection and prevention of financial crime targeted at the Bank or executed through the Bank. It is the intent of the Bank to promote consistent organisational behaviour by providing guidelines and assigning responsibility for the development and management of controls and conduct of investigations regarding financial crime. It sets out explicit steps to be taken in response to reported or suspected financial crime, as well as measures that will be takento prevent or minimise the risk of such crime. The Bank is committed to complying with applicable laws, regulations, accounting standards, internal accounting controls, and audit practices.

3. Objectives and Scope

The FC Policy establishes the Bank's framework for preventing, detecting, deterring, reporting, remediating, and punishing financial crime or dishonest activity and violations of the Code of Ethics that could create risks for the Bank or undermine the public's confidence in the integrity of Bank activities.

This Policy applies to all Exim Bank activities. In particular, it applies to the following non-exhaustivlist of persons and entities:

The members of Exim Bank Board of Directors, the Management Committee, staff and consultants, without regard to their position, rank, or length of service

- Borrowers, promoters, contractors, sub-contractors, consultants, suppliers, beneficiaries (as the case may be), and in general relevant persons or entities involved in Bank-financed activities
- Consultants, suppliers, service providers and other persons or entities procured by the Bank for its own account; and
- All counterparties and others through which the Bank deals in its activities, including, but not limited to, borrowing or treasury activities.

4. DEFINITION

What is Financial Crime?

For purposes of this Policy, financial crime is classified into three broad categories:

a) *Money laundering* is the process through which criminally derived funds or assets, including cash and securities, are moved through the global financial system to disguise their unlawful origin and/or true ownership. The funds are usually derived from illicit activities such as illegal arms sales, smuggling, organised crime, etc.

b) *Financing of Terrorism* is any funding to body (an organisation or person) that is classified as a terrorist by the competent authorities. Sources for funds for terrorism financing may be legitimate or illegitimate involve funds raised from illegitimate or legitimate sources; the criminality arises from the intended use of those funds. Typically, this involves smaller amounts than in money laundering transmitted using informally networks.

c) *Fraud* is the intentional deception made for personal gain, avoiding an obligation, or causing damage to another party. The term fraud is used todescribe offences such as, but not limited to, deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts, and collusion.

5. Board and Management Responsibilities

5.1 Board Oversight

The Board shall require regular reporting from the senior management on the assessment of financial crime risk and measures being taken to prevent financial crime in the Bank. This includes ongoing Internal Audit reports and Board Risk Committee reports, ensuring that management responses and follow-up actions to all internal and external reports that identify weaknesses in internal control policies and procedures are followed up, and associated parties given direct responsibilities for specific tasks and actions.

5.2 Senior Management

Senior Management is responsible for ensuring that the Bank has the correct policies and procedures in place to prevent the occurrence of financial crime. This includes, but is not limited to:

- Ensuring that appropriate resources and technological solutions are in place
- Ensuring that staff are trained on financial crime prevention, ethical conduct, and regulatory expectations
- Working with the Risk Management team to formulate and implementappropriate operational processes, specific to their domains, for staff to follow, and ensure they are followed in practice
- Ensuring timely follow-up and strengthening of preventive measures
- Regularly review the risks associated with the Bank's objectives
- Reviewing the policy on financial crime, including an appropriate control environment and response plans
- Establishing mechanisms for reporting suspected financial crime and issues to Risk Management
- Ensuring that swift action is taken to respond to allegations and substantiated cases of financial crime
- Make arrangements for investigating allegations of fraud, and ensuring that vigorous and prompt investigations are carried out without delay or hindrance
- Reports to the CEO or Board should further resources be required to combat fraudulent activity
- Set the overall tone to reinforce the message on the policy on financial crime

5.3 Responsibilities of the Department / Branch Heads ('Heads')

If informed of a fraud or other financial crime, Heads should listen carefully and with respect to staff, ensure that every report is treated seriously and sensitively, and give every allegation a fair hearing. Heads should obtain as much documentation and information as possible regarding the alleged fraud or other financial crime, including any notes or evidence, and they should reassure staff members that they will be protected and will not suffer any reprisal for having reported allegations made in good faith. Heads are required to prepare a written report of the details of any suspectedfraud or other financial crime that has been reported to them and provide it to the Risk Management team.

Heads should not confront the alleged perpetrator or carry out an investigation themselves. Instead, the matter should be reported immediately to the Risk Management Team, in accordance with the reporting process detailed above. No time should be lost in reporting the suspected activity.

5.4 Internal Audit

- Promote the deterrence and prevention of fraud/financial crime by evaluating the effectiveness of internal controls, and report periodically on their adequacy to the Board Audit Committee
- Review the implementation of the changes made to the system of internal control subsequent to a case of fraud to evaluate their efficiency and effectiveness

5.5 Risk Management

- Receive reports of fraud from staff and managers, and provide guidance to the CEO and senior management in determining the scope of the fraud and contacting external experts or legal authorities
- Conduct internal investigations, where applicable, including gathering evidence, conducting interviews, and writing reports on investigations
- Keep records of any allegations made, any subsequent actions taken, and the ensuing result
- Receive alerts on actual or potential money laundering/terrorism funding activities for new accounts or transactions
- Review accounts/entities or transactions and determine whether the Bank should approve/reject the account/entity or transaction
- Review and propose changes to the system of internal controls

5.6 Human Resources

- Consult with senior management regarding the appropriate disciplinary action tobe taken against the perpetrators of fraud and supervisors whose failures have contributed to the commission of fraud or those who have made frivolous or badfaith allegations
- Ensure that more detailed reference checks are carried out in recruitment processes for staff positions that may be vulnerable to opportunities for any financial crime (banking activities, procurement, etc.)
- Ensure that staff are trained on ethical issues, Code of Conduct and financial crime prevention

5.7 All Bank Staff

- Conduct themselves lawfully and properly in the use of the Bank's resources
- Remain alert to the possibility of financial crime and report suspicious behaviour to Head of Risk and Compliance who is a Bank's Money Laundering Reporting Officer (MLRO).
- If staff prefer to report anonymously they can do so through the confidential by email/Whistle blowing
- Attend a training courses on Risk Management and Financial Crime Prevention
- Sign and accept this Policy as an integral part of their employment contract withthe Bank

5.8 Content of Suspicious Report.

A suspicious report made shall contain the following information: -

a) date and time of the transaction, or, in case of a series of transactions the period over which the transactions were conducted;

b) type of funds or property involved;

c) amount or value of property involved;

d) currency in which the transaction was conducted;

e) method in which the transaction was conducted;

f) method in which the funds or property were disposed of;

g) amount disposed;

h) currency in which the funds were disposed of;

i) purpose of the transaction;

j) names of other institutions or person involved in the transaction;

k) bank account numbers in other institution involved in the transaction;

l) the name and identifying number of the branch or office where the transaction was conducted; and

m) any remarks, comments or explanation which the person conducting the transaction may have made or given in relation to the transaction

6. How Financial Crime Occurs

Financial Crime is increasing in quantity and sophistication as criminals deploy increasingly sophisticated tools and methods. Often these activities span geographies, where organised criminals hone their practices and work together to identify and exploit weaknesses in banks' defences. Thus, firms are forced to innovate continuously in order to stay a step ahead of the criminals.

Crime succeeds for a variety of reasons. One reason is due to the lack of proper internal control policies and procedures. However, even when the controls exist, they could fail because the proper procedures are not followed or are insufficiently executed. Thirdly, there might be the wrong motivation on those people charged with internal controls, including inadequate separation of duties of staff or management.

In general, crime occurs because there is an opportunity to commit the crime and there is some gain for the perpetuators. The three types of crime follow familiar patterns outlined in the table below.

Table 1: Modes of financial crime

Class	Initiation	Execution	Outcome
Money Laundering	• Select banking institutions • Develop concealment tactics • Opens account(s) and deposit funds below reportable trigger points	• Undertake a series of (possibly legitimate) financial transactions and conversions • "Wash off" source of original funds; conceal traces	• Recover funds as "clean" funds • No losses to financial firm
Terrorism Financing	• Channel raised funds into legitimate appearing conduits, e.g. charities • Select transmission mechanism	• Transfer funds to target fronting organisation, e.g. charities • Dispense funds while concealing trail of funds	• Funds transferred to terrorists • No loss to financial firm
Fraud	• Select fraud method and target victims • Develop tricks, technology and methodologies	• Extract funds directly • Divert funds midstream • Impersonate owners • Mask activities	• Direct loss to clients • Direct/indirect losses to financial firm

• Attach to "system"	

7. Guidelines

This policy is based on the following 4 guiding principles on combating financial crime:

- Individual responsibility: compliance is everyone's business. It cannot be dissociated from the exercise of any professional activity within the bank or on its behalf regardless of the mission or the Management to which each one belongs. The existence of a Compliance function within the bank shall not exempt anyone from their own personal liability in all areas of compliance.

- Completeness: compliance missions extend to all levels of the bank. To exercise them in good conditions, it must have access to all the necessary information in the different Directorates.

- Independence: the employees and correspondents of the Compliance entity within the bank carry out their missions under conditions that guarantee their independence of judgment and action.

- The rule of the "best saying" ethical: in the field of ethical standards, those adopted by the Group prevail over local rules as long as the latter are of a lower level of requirement and rigor.

8. Money Laundering and Financing of Terrorism

8.1 what the Money Laundering?

According to Article 1-1-1 of Law No. 112/AN/2011 /6th L of 25 May 2011, on Money Laundering, Confiscation and International Cooperation in relation to the Proceeds of Crime in the Republic of DJIBOUTI, are considered as money laundering, the following acts committed intentionally:

- the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;

- the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

- participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

The offences underlying money laundering are as follows:

a) any dealing which amounts to illicit drug trafficking under the law for the time being relating to narcotic drugs and psychotropic substances; terrorism, including terrorist financing;

b) terrorism, including terrorist financing;

c) illicit arms trafficking;

d) participating in an organized criminal group and racketeering;

e) trafficking in human beings and smuggling immigrants;

f) sexual exploitation, including sexual exploitation of children;

g) illicit trafficking in stolen or other goods;

h) corrupt practice;

i) counterfeiting;

j) armed robbery;

k) theft;

l) kidnapping, illegal restraint and hostage taking;

m) smuggling;

n) extortion;

o) forgery;

p) piracy;

q) hijacking;

r) insider dealing and market manipulation; or

s) illicit trafficking or dealing in human organs and tissues;

t) poaching;

u) tax evasion;

v) illegal fishing;

w) illegal mining; or

x) environmental crimes.

8.2 WHAT'S FINANCING OF TERRORISM?

Article 3 of Law No. 110/AN/11/6ème L on combating the financing of terrorism in the Republic of DJIBOUTI,

defines the financing of terrorism as any act committed by a natural or legal person who, by any means, directly or indirectly, has deliberately provided or collected property, funds and other financial resources with the intention of using them or knowing that they will be used, in whole or in part, for the commission of one or more terrorist acts by a terrorist organization, a terrorist or group of terrorists.

"*Terrorist financing*" means:

a) the provision of, or making available such financial or other related services to a terrorist, group or entity which is concerned with terrorist act; or

b) entering into or facilitating, directly or indirectly, any financial transaction related to a dealing in property owned or controlled by or on behalf of any terrorist or any entity owned or controlled by a terrorist.

8.3 AML/CTF Monitoring

8.3.1 Operational Guidelines for Customer Identification

The following operational guidelines shall apply:

a) The Bank shall institute effective procedures to establish and verify the identity of their customers at the time when the relationship is established.

b) The Bank shall further check and verify the authenticity of the submitted documents and the information tendered for the purpose of opening accounts.

c) The identity of natural persons shall be established to the Bank's satisfaction by reference to official identity papers or such other evidence as may be appropriate under the circumstances.

d) The Bank shall receive satisfactory documentary evidence of the nature of corporates, partnerships and foundations.

e) The Bank shall receive appropriate evidence of formation and existence of a Trust along with the identity of its trustees.

f) All identification documents shall be current at the time of establishing the relationship.

g) Beneficial ownership shall be established for all accounts. Due diligence shall be done on all principal beneficial owners identified.

   i) *Natural Persons*: When the account is in the name of an individual, the Bank shall establish whether the customer is acting on his/her ownbehalf. If doubts exist, the Bank shall establish the capacity in which andon whose behalf the accountholder is acting.

   ii) *Legal Entities*: Where the customer is a Company, such as a private investment company, the Bank shall understand the structure of the company sufficiently to determine the provider of funds, principal owner(s) of the shares identify the owner(s) holding at least 5% of the shares and those who have control over the funds, e.g. the directors and those with the power to give direction to the directors of the Company.With regard to other shareholders, the Bank shall make a reasonable judgment as to the need for further due diligence. This principal applies regardless of whether the share capital is in registered or bearer form.

h) The Bank shall not, in the normal course, rely on intermediaries or other third parties to perform the CDD process or to introduce business. Where suchreliance is permitted in exceptional cases, it will be kept in mind that the ultimate responsibility for customer identification and verification remains with the Bank. The criteria that will be met by such third parties are as follows:

   i) The Bank shall satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

   ii) The Bank shall satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements with the same diligence that the Bank would have employed, if the CDD was done by the Bank directly.

i) Where the holder of a power of attorney or another authorised signatory is appointed by a customer, it is generally sufficient to do due diligence on the customer. The power of attorney must meet the following criteria:

   i) Specify the name of the individual executing the power of Attorney.

   ii) The tasks and assignments to be performed should be clearly mentioned.

   iii) The power of Attorney should contain the duration/validity period in the form of completion of the task or time frame.

iv) The power of attorney should be accompanied with written instructions from the account holder. For further assurance, the it is preferable that the account holder will introduces the executor of the Power of Attorneyin person.

v) In case of a legal person issuing the power of attorney or an instructionto allow additional signatory, the power of attorney or the instruction letter should be accompanied with a board resolution signed by thedirectors and bearing the company seal.

vi) The power of attorney should be legally attested.

vii) The Bank shall then request the executor of the power of attorney to submit identification documents for him to be allowed to operate and maintain a business relationship with the Bank on behalf of the customer.

j) Any walk-in customer who would like to use the Bank for a particular transaction will be allowed to do so with the approval of the branch manager subject to meeting the banks' laid down procedure and regulatory provisions relating to walk in customers, and conducting adequate KYC procedures and CDD prior to accepting any transaction request.

k) Before opening an account with a foreign correspondent bank, the bank must ensure by all means that:

-The said correspondent is not a shell bank (a shell bank is defined as a bank that has been incorporated and licensed in a country where it has no physical presence and is not affiliated with a regulated financial group subject to consolidated and effective supervision).

-The said correspondent is subject to AML/CFT regulation that is at least equivalent to Djibouti's regulation.

l) This information collected at the time of entering into the relationship must be kept up to date throughout the duration of the business relationship.

m) The opening of an account for a correspondent bank and a PEP must be authorised by the Executive Management.

n) EXIM is must to refuse to enter into a relationship when:

- It is not in a position to identify a customer or obtain information about the subject matter of the business relationship. The Bank does not execute any transaction, regardless of the terms and conditions, and does not enter into or continue the business relationship.

- The prospect or customer is subject to a judicial ban or is on one of the sanctions lists.

Cases of refusal to enter into a relationship must be reported to the Financial Intelligence Unit of the Central Bank of Djibouti.

8.3.2 Frequency of KYC review

The client's level of money laundering and terrorist financing risk, as well as the associated due diligence and the client file, must be updated, particularly with regard to the results of the vigilance exercised by employees (relationship manager, compliance function, etc.).

8.3.3 Monitoring of transactions

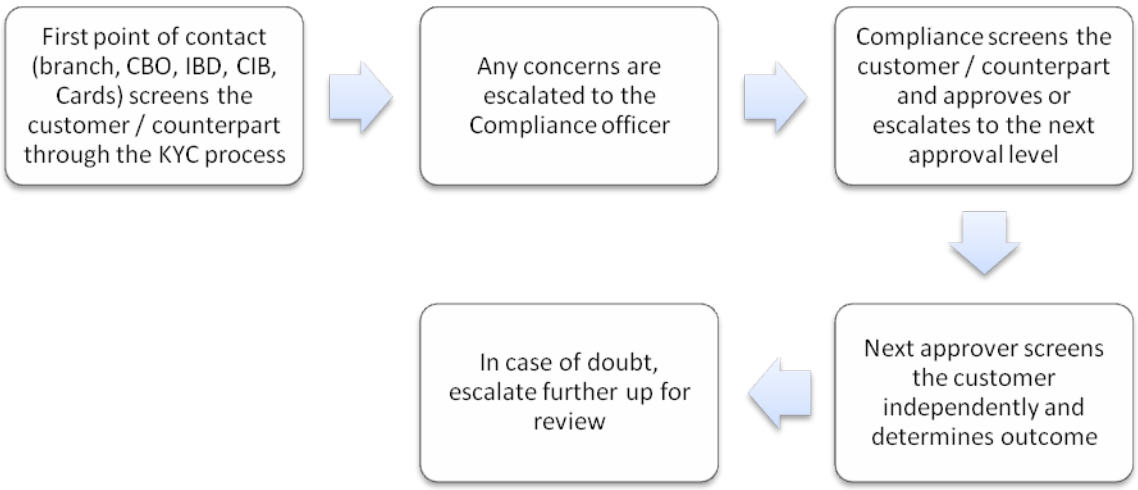
The constitution of the customer profile is based on criteria that make it possible to identify the operations expected on the customer's account (nature, frequency and amount, mode of account funding, methods of payment used, etc.).Alerts are triggered by the monitoring tool as soon as the customer acts outside his or her profile or as soon as a transaction constituting an indication of money laundering has been identified (unjustified splitting, large cash payments). All staff has a duty of vigilance regarding the customer's behaviour and suspicious movements and transactions that cannot be detected by the monitoring tools.

The Compliance Officer shall be regularly involved in the monitoring of client on boarding and transactions as an essential part of the on-going monitoring of the Bank's activities

8.3.4 Process

The Compliance Officer shall be regularly involved in the monitoring of client on boarding and transactions as an essential part of the on-going monitoring of the Bank's activities. Such monitoring shall be aimed at detecting integrity and compliance concerns that may arise during or after client acquisition.

The on-boarding screening process shall ensure the below approach for concerns escalation is in place



8.4 Risk-Based Approach

The escalation guidelines reflect the level of perceived risk. In order to define the risk level, the Bank shall use risk criteria and assign weights to each criterion. Application of risk categories provides a strategy for managing potential risks by enabling the Bank to subject customers to proportionate controls and oversight.

EBDL's risk assessment is consistent with the principles defined by the various regulations in force (FATF, national legislation, etc.), the supervisory authorities and the EBTL:
-This risk assessment analysis is based in particular on:
-Client categories
-Countries and geographical areas
-Types of products, services and operations carried out
the distribution channels
the conditions under which the operations are carried out

The risk categories will be defined by Board Risk Management Committee (B-RMC) with the support of the Risk department. BRMC shall review the rating and weight assigned to each risk category at least annually or whenever information suggests that revision is necessary

Restricted Customers and Countries

The below list is the restrictions related customers/industries and country that EBDL is prohibited to deal with by regulation, policy, and practice.
These lists refer to the 4 official sanctions lists (UN, OFAC, EU, UK) / FATF and are

updated regularly.

Customers/Industries

EDD & Restricted on a risk-based approach	Prohibited
Non-Accounts customers	Shell banks
Non-Resident Customers	Arms, Defense Military
MVTS/MSB customers	Atomic Power
PEPs	Unregulated Charities
PEP Related	Red light business/Adult Entertainment
PEP Close Associate	Virtual Currencies
Correspondent Banks	Marijuana
Extractive Industries	Gambling
Precious Metals and stones	Payment Services Provider
Regulated Charities	
Non-Governmental Organizations	
Embassies/Consulates	

Prohibited Special Risk Countries	Restricted Special Risk Countries
• Crimean Region of Ukraine • Democratic People's Republic of Korea (North Korea) • Iran • Sudan (North Sudan) • Syria • Cuba • Somalia • Yemen • Ukraine (other than the Crimean Region) • Russia	• Afghanistan • Democratic Republic of the Congo • Iraq • Lebanon • Libya • Myanmar • Pakistan • Palestine • South Sudan • Venezuela • Zimbabwe

8.5 Resourcing

At all times, the Bank shall ensure is has sufficient resources for managing AML/CTF activities. These resources shall be centralised to service all parts of the Bank. If it is determined to be necessary, dedicated resources may be deployed to a specific unit where the risk of money laundering or terrorism financing is elevated.

The Head of Risk shall have primary responsibility for determining the resource requirements and communicating these needs to the CEO and the B-RMC. On anannual basis, B-RMC shall review the resource utilisation and risk levels. Based on thatreview, the resourcing levels will be adjusted to meet the Bank's needs.

The Head of Risk shall ensure that the resources deployed to the anti-fraud programme are fit for purpose. They will have the appropriate skillsets and training to fulfil their mandate.

A simple formula may be used to determine resourcing needs. For example:

- Assume average time spent investigating incidences is 20 minutes per case perperson
- Assume that one person can deal with 10 – 18 cases per days
- Therefore, the resources needed for an average of *y* cases in a day will be *y*/10

The Bank shall continue to invest in training its employees in recognising the potential threat of money laundering transactions. Furthermore, all new employees joining the Bank shall receive extensive training on AML. The training programme shall cover areas where employees work directly with customers and / or in areas exposed to money laundering and terrorist financing.

8.6 Reporting of Suspicions

8.6.1 Cooperation with the FIU

EXIM BANK cooperates fully with the Financial Intelligence Unit (FIU) of the Republic of DJIBOUTI. This cooperation consists of:

- Informing it spontaneously and without delay when it suspects or has good reason to suspect that a money laundering or terrorist financing operation or attempt is in progress or has taken place (reporting);
- failure to identify the natural or legal person must be reported to the FIU
-
- Provide promptly, upon request, all necessary information in accordance with the procedures provided for by the applicable legislation.

Head of Risk and Compliance is a Bank's Money Laundering Reporting Officer (MLRO).

8.6.2 Professional Secrecy

The FIU Correspondent, all Compliance staff are required to respect the confidentiality of the information provided.

The client who has been the subject of a report must not be informed under any circumstances.

8.7 Archiving

All documents (client identification, operations and anti-money laundering controls, financing of terrorism, suspicious transaction reports) shall be kept in a file for each client for a minimum period of 10 years from the closing of the account or the execution of the operation.

These documents must be kept in such a way as to ensure confidentiality and to respond promptly to any request for information made by the FIU and the supervising authorities.

The documents must be kept in such a way as to guarantee their future use. The archiving criteria must be homogeneous, access must be secure, and the storage location must be appropriate

9 Fraud Management

The Bank has zero tolerance for fraudulent activity. Any act of fraud perpetratedagainst the Bank shall be cause for action by the Bank, up to and including theimmediate termination of employment or existing contractual obligations. In addition, the Bank reserves the right to pursue all appropriate legal remedies.

Management is responsible for the detection and prevention of fraud, misappropriation, and other inappropriate conduct. Each member of the management team must be familiar with the types of fraud that might occur within his or her area of responsibility and work alongside the Operational Risk Management team to periodically assess the risk of fraud, have in place and effectively maintain controls to prevent and detectfraud, and be alert for any indication of irregularity.

Any fraud that is detected or reasonably suspected must be reported immediately.

9.1 Fraud Prevention

In order to prevent fraudulent activities, the Bank shall adopt a multi-faceted strategy that encompasses cultural, organisational, process and system aspects. These are outlined below.

9.1.1 Culture

The most effective tool for preventing fraud is to instil a culture in the Bank that encourages employees at all levels to consistently execute steps that prevent or limit fraud. This cultural transformation is likely to take several years to be completed. It is the role of senior management to drive this transformation.

The ways in which the cultural transformation can be achieved include:

- Establishing an ethical framework anchored by the Code of Conduct
- Requiring all staff to comply with and to promote the Bank's ethical values with third parties
- Enforcing the Bank's ethical values consistently
- Establishing, disseminating and enforcing a clear anti-fraud policy, including sanctions for breaches
- Resolving any conflict of interest that may arise
- Training staff on anti-fraud techniques and promoting staff awareness of fraud issues
- Ensuring that new staff meet the honesty and integrity standards of the Bank
- Enhancing and maintaining staff morale and common bonds.

To effect this cultural transformation, it shall be necessary to develop fraud awareness though training programmes. The training shall cover both fraud control and ethical behaviour targeted to cover all employees. Refresher courses shall also be provided to ensure that the staff members are aware of the latest developments in fraud.

The topics that the training shall cover include (but not limited to):

- Types of fraud
- An ethical framework
- This Policy
- Anti-fraud techniques
- Alerts and reporting processes
- Responsibilities for handling allegations and inquiries into cases of fraud

- Relationship between the Policy with the Code of Conduct and professional ethics

9.1.2 Organisation

To support the prevention of fraudulent activity, the Bank shall have a centralised Fraud Prevention and Detection team. The role of this team shall be to:

9.1.2.1 Monitor the bank's activities to detect fraudulent activities including developingand implementing tools to help detect fraud;

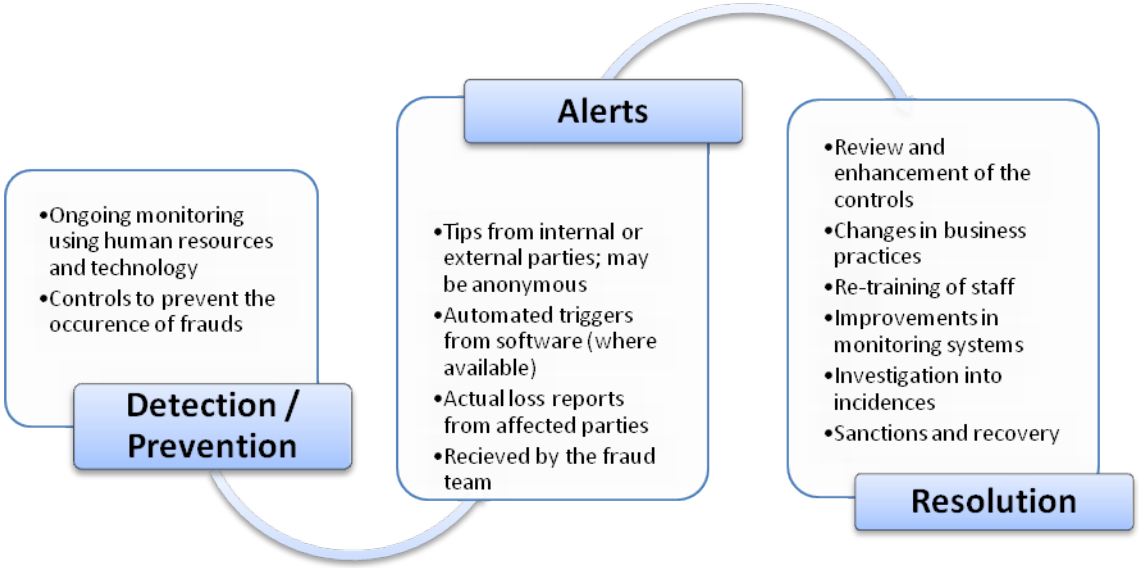
9.1.2.2 Develop and implement policies, procedures, methodologies and tools that would prevent frauds taking place.

This team shall deploy such methods and techniques that the Bank approves in order to achieve its objectives.

9.1.3 Processes and Systems

The Bank shall approve anti-fraud processes consistent with its objectives to limit and prevent fraud. These processes will be reviewed regularly to ensure that they remain effective and appropriate to the level of risk of fraudulent activities. It is the responsibility of the Internal Audit team to provide assurance that the Bank has in placeeffective anti-fraud processes.

These processes may be enabled by fraud detection software that provides for automated alerts and other tips to the fraud prevention team. To the extent possible, the Bank shall ensure that the deployed anti-fraud software is fit for purpose. The general process is shown in the diagram below.



9.2 Fraud Response

When actual or suspected fraudulent activity takes place, the Bank shall follow an effective response plan. The CEO has overall responsibility for the Bank's response. Authority for the response can be delegated to an appropriate staff member. Nonetheless, those involved in overseeing fraud response must not have any conflict of interest.

9.2.1 Early Alerts

Fraudulent activity might be detected by any member of staff or an external party. Any potential or actual fraud should be reported as soon as possible to the appropriate persons. Concerns that should be reported include, but are not limited to, the following:

9.2.1.1 Any dishonest or fraudulent act
9.2.1.2 Forgery or alteration of documents or accounts
9.2.1.3 Misappropriation of funds, supplies or other assets
9.2.1.4 Impropriety in the handling or reporting of money or financial transactions
9.2.1.5 Bribery, corruption, deception or similar activities
9.2.1.6 Unfair or illegal practices
9.2.1.7 Theft or misuse of property, facilities or

servicesWhen raising the alert, the reporter should not:

9.2.1.8 Contact the suspected perpetrator to get facts or demand restitution

9.2.1.9 Discuss the case facts or allegations with anyone outside of the Bank
9.2.1.10 Attempt to personally conduct investigations or interviews

9.2.2 Reporting Process

All staff members are obliged to report actual and suspected incidences of Fraudulent Activity as soon as it is detected. Depending on the circumstances of who is thought to be involved in the suspected fraud, staff members should report the suspected fraud to one of the following:

- The line manager(s) of the individual(s) suspected of committing fraud
- The line manager(s) is required to report the concern to the Branch/Departmental head, who will liaise with the associated Risk Officer. They will report the details to the Risk Management Department and produce a '*Risk Event Report'*
- If the line manager(s), branch/department head or Risk Officer is a potential suspect, then staff members should report the concern directly to the Risk Management Department or Internal Auditor
- If staff prefer to report anonymously, they can do so to any appropriate person, in the fraud alert email account. That person receiving the report is then charged with ensuring the information reaches the correct persons. (Refer to the Whistle-blower Policy)

All reasonable allegations will be treated seriously and systematically and will be properly investigated. Confidentiality, in so far as possible, will be maintained for all reports made in good faith, and where reports are made anonymously, such anonymity will be respected. However, if criminal activity is to be reported to the police, the identity of the person reporting may eventually have to be disclosed to enable external investigators or the police to pursue criminal investigation effectively.

If an allegation is determined to have been made frivolously, in bad faith, maliciously, for personal gain or for revenge, disciplinary action may be taken against the person making such an allegation.

9.2.3 Risk Event Report

Reports of risk incidences shall include all known details, including all individuals alleged to be involved, the location, the time, and any relevant actions or statements.

This will provide management and other associated parties with the details of any cases of fraudulent activity that occur in the Bank.

The stages for reporting following the submission of a Risk Event Report will be as follows:

From	To	Report Type	Frequency
Branches/Departments	Risk Management	Risk Event Report	At least monthly
Risk Management	CEO	Operations & Risk Subcommittee Report	At least monthly
Risk Management	Risk Management Committee	RMC Report	At least quarterly
ORC	Board Risk Committee	BRMC Report	Quarterly

9.3 Investigation

In the event of suspected or confirmed fraudulent activity, the CEO, or any person to whom such responsibility has been delegated, will initiate the formal investigation process into the matter. Typically, the responsibility will fall to the Fraud Officer, who is as part of the Risk Management Department. The Fraud Officer has the primary responsibility for the investigation of all suspected fraudulent acts. If such acts involve the Fraud Officer, the Bank's legal counsel will assign appropriate outside investigators.

In the case of complex fraudulent activity, investigations will be carried out by external parties such as external audit firms with specialized forensic accounting expertise and access to criminal law expertise, or where deemed appropriate, by the police. Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will generally be made in conjunction with the outside/contract counsel, Human Resources, and senior management, as will final decisions on disposition of the case.

Investigations shall be conducted without regard to any person's relationship to the organisation, position or length of service. The Fraud Officer shall keep records of all actions in the investigation, to ensure success in any future criminal, civil or disciplinary action. The Fraud Officer will determine who should not be involved in theinvestigation to avoid a conflict of interest situation for staff members and managers with close working relationships with the individual(s) in question.

The CEO shall ensure that full access is given to the Fraud Officer and any external body requested to assist him/her to search immediately the work area in question,

including any files and computers. All searches are to be conducted in a lawful manner, to ensure that evidence is admissible in court, if required. The Fraud Officer will keep records of any action or handling of evidence.

Interviews, if necessary, will be structured and documented as much as possible. The Fraud Officer will develop the procedure, in consultation with the Legal Adviser.

The Fraud Officer shall issue a report detailing the findings and conclusions of every concluded investigation, including recommendations for future action. Results of investigations shall not be disclosed to or discussed with any person apart from the Fraud Officer, Legal Adviser, Head Risk & Compliance, CEO, Senior Management (as appropriate), Fraud Response Team, Board, External Auditors, and anyone with a legitimate need to be involved. This is important to avoid damaging the reputation of those suspected of wrongdoing and subsequently found innocent, and to protect the civil liability and loss of reputation and goodwill.

To support the investigation process, the CEO may nominate a Fraud Response Team to coordinate responses to and remediation of fraud incidences. The guidelines for investigation are presented below.

Table 2: Guidelines on Fraud Levels

Characteristic	Level 1	Level 2	Level 3
Complexity	• Requires detailed analysis of large amounts of evidence, both paper and computer based • Use of sophisticated technology	• Requires detailed analysis of evidence, both paper and computer based	• Analysis of relevant evidence straightforward
Potential damage	• High monetary loss. Over $USD 50,000 or equivalent • Significant damage to the reputation of the Bank	• Medium monetary loss. Between $USD 5,000 and $USD 50,000, or equivalent • Significant damage to the reputation of Bank	• Minor monetary loss. Up to US $USD 5,000, or equivalent • Minor damage to the reputation of the Bank
Nature of offence	• Elements of serious criminal activity (e.g. conspiracy) • Serious breach of trust	• Likely to involve action before a court or tribunal	• Likely to be limited to administrative action within the Bank
Status of	• Preliminary	• Preliminary analysis	• Preliminary

evidence	analysis indicates strong possibility of proof beyond reasonable doubt	indicates possibility of proof to the level of proof beyond reasonable doubt or balance of probabilities	analysis indicates strong possibility of proof to the level of balance of probabilities
Availability of evidence	• Evidence is required that can only be obtained pursuant to a search warrant or surveillance	• Evidence is required that can be obtained within the Bank	• Evidence is required that can be obtained within the Bank
Scope	• Involves known or suspected criminal activities in a number of agencies and/or jurisdictions • Collusion between a number of parties	• More than one party suspected of being involved in the case	• Isolated incident

Based on the guidelines in Table 2, the following shall be part of the Fraud Response team:

Fraud Level	Fraud Response Team
Level 1	CEO (or designate), Head of Operations, Risk, Internal Audit, HR, Legal (external), External Investigators
Level 2	CEO (or designate), Head of Operations , Risk, Internal Audit, HR
Level 3	Senior Management, Risk, Internal Audit, HR

9.4 Outcomes

Where the investigation reveals that a staff member has committed fraudulent activity, the Bank's disciplinary procedures will be applied. In certain cases, the CEO, in consultation with the Legal Adviser, the Head of Risk & compliance and the Head of Human Resources, may direct that legal action be undertaken. Where appropriate, criminal prosecution should be pursued. Otherwise, depending on the nature of the case, one or more of the following options may be applied, consistent with the perpetrator's relationship with Bank and the rights and obligations therein under applicable law:

- Counselling
- Loss of privileges
- Greater scrutiny or increased controls
- Transfer to another area

- Demotion
- Suspension
- Termination
- Summary dismissal

Disciplinary action may also be brought against supervisors whose failures have contributed to the commission of fraud or a staff member deliberately making an allegation in bad faith.

Follow-up Action

Following a case of fraud, the CEO shall ensure that all managers and staff in the affected area are debriefed on the process and outcome of the investigation. There should also be a follow-up with the individual(s) who reported the initial suspicion of fraud, to provide assurance that their claims have been taken seriously.

Depending on the circumstances, the CEO may consider the need for communication with staff on a larger scale. The CEO shall ensure that the organisation conducts a thorough review of operating procedures in the areas affected by the fraud and that improvements are made where necessary. Lessons learned shall be disseminated throughout the organisation, where applicable, to strengthen the system of internal control and to foster an anti-fraud culture. A report on actions taken shall be submitted to the BRMC.

9.5 Resourcing

The Bank shall have sufficient resources to managing anti-fraud activities. These resources shall be centralised to service all parts of the Bank. If it is determined to be necessary, dedicated resources may be deployed to a specific unit where high incidences of fraud are occurring or could occur.

The Head of Risk shall have primary responsibility for determining the resource requirements and communicating these needs to the CEO and BRMC . On an annual basis, the CEO and the BRMC shall review the resource utilisation and risk levels. Based on that review, the resourcing levels shall be adjusted to meet the Bank's needs.

The Head of Risk shall ensure that the resources deployed to the anti-fraud programme are fit for purpose. They will have the appropriate skillsets and training to fulfil their mandate.

10 Related Policies for Further Guidance

This Policy document should be read, applied in conjunction, and consistent with the following resources:

- Whistle-blower Policy
- Code of Conduct
- Human Resources Policy
- Conditions of Service
- Accounting Standards and Procedures

11 Revision and Annual Review

This Policy shall be revisited and reviewed/updated at least once on an annual basis, or earlier depending on exigencies.

12 Effective Date

This Policy shall be effective from the date approved by the Board.
Approval Date: 30 June 2020

CHAIRMAN	
DIRECTOR	
CEO	
CHIEF RISK OFFICER	

13 Appendix: Definitions

11. 1 Financial Crime

In pursuance of this Policy, **Financial Crime** includes corruption, fraud, coercion, collusion, obstruction, money laundering and financing of terrorism defined as follows:

- *A corrupt practice*, which is the offering, giving, receiving, or soliciting, directly or indirectly, anything of value to influence improperly the actions of another party.
- *A fraudulent practice*, which is any act or omission, including a misrepresentation that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation.
- *A coercive practice*, which is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party.
- *A collusive practice*, which is an arrangement between two or more parties designed to achieve an improper purpose, including influencing improperly the actions of another party.
- *An obstructive practice* is
    a) deliberately destroying, falsifying, altering or concealing of evidence material to the investigation; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation, or
    b) acts intended to materially impede the exercise of the Bank's contractual rights of audit or access to information or the rights that any banking, regulatory or examining authority or other equivalent body may have in accordance with any law, regulation or treaty or pursuant to any agreement into which the Bank has entered in order to implement such law or regulation