የኢትዮጵያ ብሔራዊ ባንክ
NATIONAL BANK OF ETHIOPIA

LICENSING AND SUPERVISION OF BANKING BUSINESS

INTERNAL CONTROL AND RISK MANAGEMENT OF BANKS
DIRECTIVE No. SBB/XX/2025

Table of Contents

PREAMBLE 4

1. Short Title 5

2. Definitions 5

3. Scope 9

4. Internal Control System 10

4.1 Architecture and Functionalities of the Internal Control System 10

4.2 The Accounting Control System 12

4.3 Information and Technology Security Management 14

4.4 The Documentation and Information System 17

5. First Line of Defense Control 17

5.1 General Principle 17

5.2 Exercise of Control 18

5.3 Implementation 18

6. Second Line of Defense Control 19

6.1 Components of Second Line of Defense 19

6.2 Risk Management as a Component of Second Line of Defense 19

6.3 Compliance Function as a Component of Second Line of Defense 21

7. Third Line of Defense Control 25

7.1 General Principle 25

7.2 Responsibilities of Internal Audit Function 26

7.3 Audit of Other Control Functions 26

7.4 Reporting 27

7.5 Coordination of Internal Audit with the Compliance Function 28

8. Governance of Internal Control and Risk Management System 28

8.1 Role of the Board of Directors 28

8.2 Role of Senior Management 29

9. Shari'ah Governance Framework 30

9.1 Shari'ah Committee 30

9.2 Shari'ah Compliance Function 31

9.3 Shari'ah Audit Function 31

10. Risk Management 32
10.1 General Provisions for Risk Management 32
10.2 Risk Appetite Statement 33
10.3 Risk Strategy 35
10.4 Risk Policies 40
10.5 Risk Reports 45
11. Additional Requirements for Specific Risks 45
11.1 Credit Risk Management 45
11.2 Market Risk Management 54
11.3 Operational Risk Management 56
11.4 Liquidity Risk Management 61
11.5 Concentration Risk Management 67
11.6 Management of Interest Rate Risk in the Banking Book 68
11.7 Other Risks 69
12. Repeal 69
13. Effective Date 69

PREAMBLE

WHEREAS, it is necessary to promote a sound risk management culture and reinforce the internal control and risk management systems of banks in view of ensuring the stability of the banking system;

WHEREAS, the National Bank is committed to implement international standards in terms of internal control and risk management, in particular the Basel Committee on Banking Supervision Core Principles for Effective Banking Supervision;

WHEREAS, the National Bank intends to further enhance and reinforce its risk-based approach, which requires that in banks, the management, control and audit of risks are ensured by different lines of defense in the arrangement of internal controls and where, in addition, the risk management shall be ensured within a framework where general principles are respected;

NOW, THEREFORE, in accordance with Article 91(2) of the Banking Business Proclamation 1360/2025, the National Bank of Ethiopia has issued this Directive.

1. Short Title

This Directive may be cited as **"Internal Control and Risk Management of Banks Directive No. SBB/XX/2025".**

2. Definitions

For the purpose of this Directive, unless the context requires otherwise:

2.1 **"Bank"** means a private or state-owned bank, a foreign bank subsidiary or a branch of a foreign bank licensed by the National Bank to undertake banking business;

2.2 **"Bank Group"** means both domestic and foreign bank and all its subsidiaries, branches, affiliates and holding company, wherever located, that the National Bank determines to be taken into account for the purpose of implementing this Directive;

2.3 **"Board"** means the governing body of a bank appointed by shareholders or other authorized body that has primary accountability for the governance and performance of the bank including strategy, overseeing management and protection of the shareholder and stakeholder interests;

2.4 **"Chief Executive Officer"** means a person, by whatever title that person may be referred to, who is primarily responsible for the day-to-day management of the affairs of a bank;

2.5 **"Concentration Risk"** means the risk caused by the business of a bank focusing on a customer (including group of connected counterparties and related parties), partner, product, transaction, sector, economic field, currency, geographical area, to the point of causing significant impact to income, capital and risk position, as specified in the bank's internal policies;

2.6 **"Conflict of Interest"** means a situation where an individual or department of a bank makes decisions within their competence that are not appropriate for or go against interests of the bank and that benefit an external party;

2.7 **"Control Culture"** means the cultural value of a bank showing unity in awareness of risk control and management among the board, senior management, individuals and departments. The control culture is created from work ethics, internal policies and reward/disciplinary schemes to encourage individuals and

departments to actively identify and control risks in their own activities as well as the commercial banks/foreign banks' branches;

2.8 **"Credit Risk"** means the potential that a bank borrower or counterparty will fail to meet its obligations in accordance with agreed terms. This definition is applicable to interest-free banks managing the financing exposures of receivables and leases (for example, Murābahah and Ijārah). Credit risk also includes the risk arising in the settlement and clearing transactions by the counterparties on the market;

2.9 **"Credit Risk-Bearing Decisions"** means decisions of a bank in credit activities, including at least: credit granting decisions; credit limit decisions; limit-exceeding loan decisions; loan term restructuring decisions; loan group transfer decisions;

2.10 **"Credit Requiring Attention"** means exposures of a bank belonging to asset classification categories of "special mention" or above (substandard, doubtful or loss), as stipulated in the relevant National Bank Directive and subject to enhanced monitoring under the conditions defined by banks;

2.11 **"Director"** means any member of the board of directors of a bank, by whatever title the person may be referred to;

2.12 **"Economic Capital"** means the capital level determined by a bank for addressing its risks as defined by the relevant National Bank Directive;

2.13 **"Financial Institution"** means a bank, an insurance company, a reinsurer, a microfinance institution, a micro insurance company, payment instrument issuer, payment system operator, a capital goods finance company, a money transfer institution, a postal money transfer institution or such other similar institution as determined and licensed by the National Bank;

2.14 **"Group of Connected Counterparties"** means a group of counterparties with specific relationships of control or economic interdependence, such that, if one of the counterparties were to fail, all of the counterparties would be likely to fail, as defined by the relevant National Bank Directive;

2.15 **"Internal Control System"** means a combination of mechanisms, processes, internal policies, and organizational structures of a bank which follows the provisions of the Banking Business Proclamation No. 1360/2025;

2.16 **"Interest-Free Bank"** means a bank licensed by the National Bank to engage in interest-free banking services;

2.17 **"Interest Free Banking Service"** means provision of banking service by a full-fledged interest free bank or interest free banking service window in compliance with Shariah principles, including non-acceptance of interest;

2.18 **"Lines of Defense"** means the components of the internal control system of a bank. The first line of defense is made of the controls conducted by the operational risk-taking functions of a bank, through processes such as validation, peer reviews, management reviews and other due diligences incorporated into operational processes. The second line of defense is made of the controls conducted by the risk management function of a bank, which is an independent unit not related to the risk-taking units and reporting directly to the board. The third line of defense is made of the controls conducted by the internal audit, which is an independent function of a bank, not related to the risk-taking units and to the second line of defense, and which reports to the board through the internal audit committee;

2.19 **"Liquidity Risk"** means the risk caused by:

2.19.1 the banks' inability to fulfil debt obligations at maturity, including the banks' inability to honor its payment obligations in RTGS and other settlement systems; and/or

2.19.2 the bank being able to fulfil debt obligations at maturity, but at higher costs than the average market costs, as specified in the bank's internal policies.

2.20 **"Market Risk"** means the risk of losses in on- and off-balance sheet positions arising from adverse movements in market prices i.e. fluctuations in values in tradable, marketable or leasable assets and in off-balance sheet individual portfolios. Market risk may be stemming from FX, commodities, equity or interest rates fluctuations;

2.21 **"Material Activities"** means activities designated by a bank, as important for their business model and that may have a significant impact on the financial performance in accordance with the bank's internal policies;

2.22 **"Material Risks"** means risks that may have a significant impact on the profitability or the capital situation of a bank;

2.23 **"National Bank"** means the National Bank of Ethiopia.

2.24 **"Non-executive Director"** means an individual not involved in the day-to-day management and not a full-time salaried employee of a bank or of its subsidiaries;

2.25 **"Operational Risk"** means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements;

2.26 **"Outsourcing"** means the bank (hereinafter referred to as the client) making an agreement in writing (an outsourcing contract) on hiring another enterprise, bank or non-bank institution, domestic or foreign (hereinafter referred to as the contractor) to carry out one or multiple activities (including data processing or some steps of the business process) in the bank's stead, in accordance with the relevant National Bank Directive;

2.27 **"Regulatory Capital"** means the minimum required capital as defined by the relevant National Bank Directive;

2.28 **"Related Party Transaction"** means any transaction with related parties as defined by the relevant National Bank Directive;

2.29 **"Risk"** means the probability of loss (financial or non-financial), causing decrease in the bank's own capital and income, hence decreasing the capital adequacy ratio or hindering the bank from achieving its business goals;

2.30 **"Risk Appetite"** means the risk level that a bank is willing to take during implementation of its business strategies. Such a definition of quantitative and qualitative objectives is also referred to as a statement of direction, specifying the level of risk exposures that the bank is willing to take on in defined circumstances. An effective risk appetite considers the existing risk profile, and the capacity and willingness to assume each risk in respect of each segregated part of the bank;

2.31 **"Risk Appetite Statement"** means the document describing the risk appetite of a bank and approved annually by the bank's board of directors;

2.32 **"Risk-Bearing Decisions"** means decisions of a bank's competent level that create risks or change the bank's risk position;

2.33 **"Risk Management"** means a process of identification, measurement, monitoring and control of risks in a bank;

2.34 **"Risk position"** means a bank's risks of all types resulting from the assets, liabilities and off-balance sheet items. The risk position reflects at each moment in time the magnitude of the credit, market, operational and other risks taken for the implementation of the risk appetite of the bank;

2.35 **"Risk Policies"** means the set of rules related to the risks borne by a bank. Risk policies include risk-taking policies and risk-management policies;

2.36 **"Risk-Taking Policies"** means the set of rules and principles established by a bank's senior management to organize the execution of the risk appetite statement decided by the bank's board of directors. It includes the rules of delegation granted to the operational functions, the limits of risk-taking and the decision process for engaging the funds and responsibility of the bank;

2.37 **"Shari'ah Committee"** is a group of experts of a bank that provides interest-free banking services; having knowledge of the Shariah principles and banking business; and is responsible for ensuring that the bank's products and services are in compliance with Shariah principles;

2.38 **"Senior Management"** means the chief executive officer, the senior executive officers, and any other official, as may be defined by individual bank, responsible for day-to-day running of a bank;

2.39 **"Stress Test"** means an assessment of volatilities and unfavorable developments' impact on the capital adequacy ratio and liquidity and other critical financial indicators in various scenarios in order to determine a bank's resistance;

3. Scope

This Directive shall be applicable to all banks operating in Ethiopia and, where applicable, on a consolidated basis for bank group.

4. Internal Control System

4.1 Architecture and Functionalities of the Internal Control System

4.1.1 Responsibility

a) Internal control system of a bank shall be determined by the bank's board and implemented by the bank's senior management in accordance with the requirements of the National Bank. It shall include three lines of defense with the functionalities defined in this Directive.
b) As a general rule, the first line of defense controls and compliance controls (as part of the second line of defense controls) cannot be outsourced. Other components of the internal control framework may be outsourced in accordance with the provisions of the relevant National Bank Directive, but their architecture, functionalities, performance and results shall remain under the responsibility of the bank.

4.1.2 Role of the Internal Control System

A bank shall put in place an internal control system which allows the bank to ensure the following, in optimum conditions of security, reliability and completeness:

c) compliance of the operations carried out, the organization and the internal procedures, with the legal and regulatory requirements in force, the professional and ethical standards and practices, as well as with the internal policies and procedures;
d) strict compliance with decision-making and risk-taking policies and procedures, as well as internal standards and limits;
e) quality and timeliness of accounting and financial information for the bank's board and management, the National Bank, or intended to be published;
f) conditions of evaluation, recording, conservation and availability of this information, particularly the existence and quality of the audit trail;
g) quality of information and communication systems; and
h) implementation within a reasonable timeframe of the corrective measures to remedy the findings made by the various internal control functions or the National Bank.

4.1.3 Proportionality

a) A bank shall ensure that the structure and size of its internal control

system are commensurate with the bank's size, complexity, risk profile and business model, as determined by its senior management and approved by the board.

b) Where applicable, a bank shall take into account the internal standards of the bank group to which it belongs, while ensuring that the provisions adopted comply with the provisions of this Directive.
c) Where applicable, a bank's subsidiaries shall include in their internal control system, the standards they define, so as to ensure effective monitoring of risks on a consolidated basis, while remaining in compliance with the provisions of this Directive.
d) A bank wishing to apply the principle of proportionality for any exception to the application of the requirements of this Directive, shall seek the approval of the National Bank. The proposed framework shall provide reasonable guarantee of effective control.

4.1.4 Interest-free banking specificities

A bank offering interest-free banking services shall also ensure internal systems, procedures and controls as set out in this Directive, proportionate to their size, to provide reasonable assurance that:

a) the transactions and dealings of the bank or window are in compliance with Shari'ah rules and principles;
b) appropriate risk management policies and practices are followed; and
c) interest-free banking business and conventional banking business are properly segregated.

4.1.5 Segregation of Functions

a) A bank shall ensure a strict separation of first, second and third line of defense control functions.
b) Within the second line of defense control, a bank shall ensure a strict separation between the functions of compliance and of risk management. When the size of the bank does not justify entrusting the responsibility for these second line of defense control functions to different people, a bank shall seek prior authorization from the National Bank to merge these functions. In no case, the first line of defense and third line of defense controls may be merged with another level of control.
c) The bank's processes for carrying out operations shall include appropriate first and second line of defense procedures to ensure the

regularity, reliability and security of these operations.

d) The control procedures shall be determined according to the type and level of risks inherent in the operations. Areas which present potential conflicts of interest or the risk of overlapping competences or responsibilities shall be identified, subject to enhanced monitoring and regular assessment with a view to resolving these conflicts.

4.1.6 Hierarchical Level

a) The responsibility for second line of defense and third line of defense control functions shall be entrusted to a senior executive officer in accordance with the relevant National Bank Directive, presenting all the guarantees of morality, integrity, competence and professional experience; their hierarchical position in the organization chart of the subject banks shall give them the necessary authority to make any remark or observation about the operational functions.

b) In any case, they shall have a hierarchical rank immediately below the bank's board. They shall report to the board and to relevant board committees to ensure their independence.

4.1.7 Procedures

a) A bank shall draw up and keep up to date manuals of procedures relating to the bank's activities. These manuals shall be periodically reviewed, at least every two (2) years. These documents shall describe the procedures for recording, processing and reporting information, the accounting schemes and the procedures for initiating and monitoring operations.

b) Each service or operational unit belonging to the internal control system shall have a regularly updated manual to perform their tasks. These manuals shall be endorsed by the senior management after approval by the board, and circulated to the relevant staff on a "need-to-know" basis.

4.2 The Accounting Control System

4.2.1 Accounting Information

A bank shall put in place a control system for accounting of transactions that enables the bank to ensure the reliability and exhaustiveness of the recording of its accounting and financial data and to ensure the availability of information according to the regulatory requirements of the National Bank, the International Financial Reporting Standards or

their own chart of accounts prepared in line with standards widely accepted internationally.

4.2.2 Accounting Procedures

a) A bank's methods of recording transactions in the financial statements shall provide for a set of procedures guaranteeing the audit trail, allowing:

   i. reconstructing the set of operations in chronological order;

   ii. justifying any information by an original document from which it shall be possible to go back by an uninterrupted progression to the summary document and vice versa; and

   iii. explaining the evolution of accounting balances from one closing to another by keeping the record of movements that affected the accounting items.

b) Any exception to the preceding principles, as regards the justification of an accounting balance or the publication of information, shall be the subject to a detailed justification, published in the appendix to the financial statements and approved by the external auditors.

4.2.3 Justification of prudential Requirements

a) The information contained in a bank's financial statements and that is necessary for the calculation of impairment, provisioning, and prudential ratios, shall comply with the provisions of the relevant National Bank Directives.

b) A bank shall be able to justify each of the amounts entered with documents having sufficient probative force.

4.2.4 Securities and Other Assets in Custody

a) Any securities and other assets held or managed by a bank on behalf of third parties shall be closely monitored through an accounting system, which retraces accurately inputs, outputs, and stocks and makes the object of internal controls and periodic inventories.

b) A distinction shall be made between securities received on free deposit and those serving as guarantees in favor of the bank itself or of third parties. The values assigned as collateral shall be duly recorded in the accounting system.

4.2.5 Reliability

A bank shall ensure the completeness, quality and reliability of the information and methods of valuation and accounting for transactions, in particular by means of the following provisions:

a) control the adequacy of the methods and parameters used for the assessment of operations;
b) regular accounting and processing information in light of principles of general prudence, loyalty, sincerity and security and compliance of the accounting schemes with the rules in force; and
c) for transactions that involve exchange rate risks or other market risks, regular reconciliation, at least on the month-end closing date, shall be performed between the results calculated by the operating units and the accounting results obtained based of the applicable valuation methods. Any significant deviations observed shall be justified and brought to the attention of the senior management.

4.2.6 Record keeping

a) For the purposes of the examinations to be carried out by the National Bank, a bank shall keep all the files and the documentation necessary to justify their accounting balances.
b) This provision applies without prejudice to other legal and regulatory provisions in force relating to confidentiality and retention of information.

4.3Information and Technology Security Management

4.3.1 Principle

a) A bank shall determine the level of information technology (IT) security needed in relation to the requirements of their activities. The bank shall ensure that the level of security is approved by the board and that the information systems are adapted to the risks inherent in the bank's operations and to the characteristics of the bank.
b) A bank shall ensure that its information control systems address the following:
    i. the level of security of the IT systems is periodically assessed and, if necessary, corrective actions are taken to reduce identified risks;

ii. IT back-up procedures are available to ensure business continuity in the event of serious difficulties affecting the operation of IT systems; and

iii. conservation of information and the documentation relating to analysis, programming and execution of any activity.

4.3.2 Governance

a) Based on the recommendation of its senior management, a bank's board shall approve the IT strategy and operational plan, including the budgets allocated to it. Likewise, the board shall approve the cyber security policy.

b) The board shall ensure that the senior management has clearly defined the roles and responsibilities assigned to the heads of the IT development and production functions (systems and networks), as well as to the head of the security of the information, which are designated according to competence criteria. These functions shall be segregated, unless the size of the bank does not allow such segregation. In this case, the specific organization shall be submitted to the approval of National Bank.

4.3.3 Internal Control of the information system

a) A bank shall ensure that, at a minimum, its internal control framework for information system includes:

i. arrangements and resources, which are implemented effectively promote the sound management, functioning and security of the information system;

ii. information systems are organized in an orderly and efficient manner, based on mapping of applications, systems and networks;

iii. new projects or equipment are deployed on time and within defined budgets and meet user needs;

iv. the functioning of the information system is carried out under conditions of satisfactory availability and incidents are minimized;

v. a business continuity plan is operational and allows business to continue under satisfactory conditions for users; and

vi. the information system manages and produces reliable data, which can be an effective basis for risk management.

b) These actions shall be conducted on an on-going basis by the second line of defense as part of its daily activities, by means of reports, watch lists or performance indicators; and shall be conducted periodically by the third line of defense, in the form of audits.

4.3.4 IT Security

a) Responsibility for a bank's information security shall rest with a dedicated function (information security function - ISF), independent from the operational unit in charge of the management and daily operation of the information system.
b) The ISF shall report to the head of the second line of defense. In the absence of an assigned information security officer, if the size of the bank does not justify it, the risk management function assumes directly this role of ISF.
c) The ISF shall ensure that IT security issues are properly handled and organized within the bank based on rules, the implementation of which it supervises.
d) Changes to the information system (projects, use of new techniques, outsourcing) shall be systematically subject to security analyses which are submitted to the ISF.
e) The ISF shall ensure that the hardware equipment of the information system is subject to adequate protection against intrusion or destruction attempts, which covers both physical security issues (protection operating premises) and logical security issues (protection of environments, communications and data). The management of access and the authentication of users of the information system shall be included as essential elements for this protection.
f) The ISF shall ensure that confidentiality of data is protected, which is based on a classification of their level of sensitivity and protection solutions, and assumes that detection mechanisms are used to detect abnormal actions on the systems and the data, in particular in with a view to detecting potential acts of internal or external fraud. This shall include analysis and implementation of IT security tools and methodologies, such as two factors authentication systems, encryption, cyber risk protection and others.

4.4 The Documentation and Information System

4.4.1 General Principle

a) A bank shall establish and keep up to date an Internal Control Charter, which specifies the mechanisms to ensure the proper functioning of the internal control system, and in particular:
   i. the different levels of responsibility;
   ii. the powers vested and the resources allocated to the operation of the internal control system;
   iii. the rules which ensure the independence of the functions under the conditions provided for in this Directive;
   iv. procedures relating to the security of information and communication systems and to business continuity plans;
   v. a description of the systems for measuring, limiting, monitoring and controlling risks; and
   vi. the method of organization and operation of the compliance control system.

b) The documentation shall be organized in such a way that it can be made available, at their request, to the board, the senior management, the audit committee, any other governance committees, external auditors and the National Bank.

4.4.2 Documentation Control for a Bank under a Bank Group

A bank belonging to a bank group, that it is established in Ethiopia or abroad, shall have available in at premises in Ethiopia all documents related to audits, controls, policies and procedures, internal control and risk management, established at group level. These documents shall be written in English as working language, and shall be provided to National Bank as requested.

5. First Line of Defense Control

5.1 General Principle

5.1.1 A bank's heads of business units are the first line of defense. They take risks and are responsible and accountable for the ongoing management of such risks. This includes identifying, assessing and

reporting such exposures, taking into account the bank's risk appetite and its policies, procedures, internal limits, and controls.

5.1.2 The manner in which the business units execute their responsibilities shall reflect the bank's existing risk culture.

5.1.3 The board shall promote a strong culture of adhering to limits and to the management rules of risk exposures.

5.2 Exercise of Control

5.2.1 A bank shall put in place, in each business unit, a first line of defense control function, responsible to ensure daily the processing operations according to principles and procedures defined by the senior management. A bank shall guarantee the segregation of functions (for example, commitment of operations, validation, accounting recording, payment, and reconciliation) and the compliance with the bank's risk-taking policy.

5.2.2 The procedures shall provide how the first line of defense controls are conducted under the surveillance or by the heads of business units.

5.3 Implementation

5.3.1 A bank's first line of defense controls shall be carried out as follows:

a) primarily by business unit managers;
b) if necessary, by separate operational attendants, in the form of cross-checks;
c) or by the operational teams themselves as part of their usual activities in order to ensure the traceability of their actions; and
d) if necessary, in an automated manner, using functionalities provided for this purpose in the IT systems.

5.3.2 The control processes shall be organized in a manner that ensures segregation of conflicting functions, under the conditions set out under Sub-Article 5.2 of this Directive.

5.3.3 The traceability of the first line of defense controls shall be ensured according to the appropriate specifications defined by the bank.

6. Second Line of Defense Control

6.1 Components of Second Line of Defense

6.1.1 A bank's second line of defense shall be organized under the responsibility of a Chief Risk and Compliance Officer into two functions with different roles and responsibilities:

a) risk management function;
b) compliance function.

6.1.2 In small banks, these functions may be combined under the proportionality conditions provided for under Sub-Article 4.1.4 of this Directive.

6.2 Risk Management as a Component of Second Line of Defense

6.2.1 General Principle

a) A bank shall, in accordance with procedures adapted to their size, their risk profile and the nature of their activities, determine the framework for risk management and organize the second line of defense independently from the functions subject to these control activities.
b) The bank's framework for risk management shall consist of procedures, tools and systems, implemented to ensure the reliability, accuracy and security of the operations conducted by the business units. It includes the tools, watch lists, loss monitoring systems, limits monitoring systems and other surveillance devices implemented in compliance with the risk strategy of the bank.
c) The second line of defense shall be implemented within the risk management function and shall ensure that the first line of defense controls are efficient and that the overall risk-taking practice of the bank is compliant with the risk appetite approved by the board.

6.2.2 Responsibility of the Chief Risk Officer

a) The risk management responsibility shall be entrusted to a chief risk officer, senior officer who coordinates his daily activity and actions with the CEO and with direct access to the bank's board of directors, as well as the bank's risk management and compliance committee.
b) The risk management function shall submit quarterly reports to the board, summarizing the actions and findings of the second line of defense, as stipulated under Sub-Article 6.2.7 of this Directive.

6.2.3 Expertise and Role

A bank's chief risk officer and other officers of its risk management function shall have the appropriate expertise to control all activities. The activities shall be periodically audited by the third line of defense.

6.2.4 Bank Group Policy and Outsourcing

The second line of defense and third line of defense controls may be outsourced within the group and entrusted to pooled central functions. However, such outsourcing shall meet the conditions of the relevant National Bank Directive.

6.2.5 Appointment of Chief Risk Officer

The conditions for the appointment and dismissal of a bank's chief risk officer shall be as provided for by the relevant National Bank Directive.

6.2.6 Responsibilities of a Bank's Risk Management Function

a) Key activities and responsibilities of a bank's risk management function shall include, among others:
   i. identifying material individual, aggregate and emerging risks;
   ii. assessing these risks and measuring the bank's exposure to them;
   iii. subject to the review and approval of the board, developing and implementing the enterprise-wide risk management framework, which includes the bank's risk culture, risk strategy, risk appetite and risk limits;
   iv. on-going monitoring of the risk-taking activities and risk exposures in line with the board-approved risk appetite, risk limits and corresponding capital or liquidity needs (i.e. capital and liquidity planning);
   v. establishing an early warning or trigger system for breaches of the bank's risk appetite or limits;
   vi. influencing and, when necessary, challenging decisions that give rise to material risk;
   vii. reporting to senior management and the board or the risk management and compliance committee on all these items, including but not limited to proposing appropriate risk-mitigating actions;
   viii. ensuring the proper execution of the first line of defense

controls;

ix. ensuring the proper implementation of corrective measures decided in response to third line of defense recommendations or by the National Bank.

b) The findings made by a bank's second line of defense shall be formalized, traceable and auditable. The findings shall be communicated to the operational units concerned so that corrective measures can be taken without delay.

6.2.7 Reporting

a) A bank's quarterly risk management report" shall include at least:
   i. main evolutions on the level of risks linked to the activity;
   ii. main findings on the assessment of the risks linked to new products or new activities;
   iii. main breaches of limits and mitigation actions;
   iv. main results of the monitoring of first-level controls;
   v. results of the stress tests conducted;
   vi. status of the implementation of the recommendations issued by internal or external auditors and the National Bank, on the internal control framework; and
   vii. any other issue of interest for the bank's board.

b) In the event of persistent failure to implement corrective actions recommended at the end of its checks, the risk management function (or, where existent the chief risk officer) shall submit to the board and to the senior management, a special report according to the procedures defined by the bank.

6.3 Compliance Function as a Component of Second Line of Defense

6.3.1 General principle

a) An independent compliance function is a key component of banks' second line of defense. This function is responsible for, among other things, ensuring that a bank operates with integrity and in compliance with applicable laws, regulations and internal policies.

b) A bank shall set up a compliance function, responsible for ensuring

the compliance of operations with the rules of professional conduct and ethics defined by the board. These rules shall be formalized in an ethics charter or a code of ethics distributed to all staff.

c) The compliance function shall have sufficient authority, stature, independence, resources and access to the board. Management shall respect the independent duties of the compliance function and not interfere with their fulfilment.

6.3.2 Organization of the Compliance Function

The organization of a bank's compliance function shall respond to the following conditions:

a) the compliance function reports directly to the head of compliance or chief risk officer (where risk and management functions are combined) and has access to the bank's board of directors and in particular to the risk management and compliance committee;
b) the compliance control function coordinates its daily activity and actions with the senior management (CEO) in accordance with the CRO's instructions, without, however, having any link of subjection with the CEO;
c) the compliance function coordinates the management of the compliance risk (including Shari'ah non-compliance) within the bank;
d) the compliance function is independent of the operational units; and
e) the head and the staff of the compliance function shall have a high level of competence in the field of banking and financial activities and an in-depth knowledge of the rules and standards in force.

6.3.3 Appointment of Head of Compliance

In line with the relevant National Bank Directive, a bank's board's prior consent, among other, is required for the following decisions:

a) the appointment of the head of the compliance function;
b) the revocation or termination of the functions of the head of the compliance function;
c) the determination of the remuneration of the function responsible for the control of compliance. This shall not depend on the performance of the business unit subject to the compliance control.

6.3.4 Termination

a) Any measure of revocation of the person in charge of controlling compliance shall be the subject of ex post information, together with a supporting file, to the National Bank showing the reasons for said measure. The dismissal can only take place after the assent of the

board, after having obtained the opinion of the audit committee.

b) An abusive dismissal measure taken without respecting the provisions of this article is liable to sanctions.

6.3.5 Bank Compliance Policy and Charter

The compliance control policy shall identify the fundamental aspects of the compliance risk, define the role and objectives of the compliance function and set up a continuous training program for staff and managers. This policy shall also provide for the development of a compliance charter which:

a) sets out the objectives of the compliance function, establishes its independence and defines responsibilities and powers;
b) describes the relations with other functions in charge of control;
c) grants the compliance control function the right of access to any information necessary for the performance of its duties;
d) gives the compliance function the right to initiate any useful investigation;
e) establishes the right and modalities to report to the senior management and, where appropriate, to the relevant board committees; and
f) defines the terms and conditions under which the compliance function may have recourse, if necessary, to external experts.

6.3.6 Responsibilities of the Compliance Function

The compliance function shall be responsible for:

a) the identification of standards governing the exercise of the bank's activities, in particular all legal risks. These standards shall be communicated to all staff.
b) the identification and the assessment of the compliance risk inherent in the bank's business model. To this end, it establishes procedures for:
    i. compliance of the operations carried out with the rules and standards in force;
    ii. identification and measurement of the compliance risks inherent in any new type of activity, product, customer major transformation of existing products, as well as exceptional operations, and reporting the assessment to the senior management and to the board; and
    iii. permanent monitoring of modifications or changes that may

occur in the texts applicable to the operations carried out by the bank.

c) the formalization of compliance procedures policies;
d) the coordination of the implementation of the national framework against money laundering and terrorist financing (AML/CFT), including laws, regulations and standards acknowledged by the Ethiopian authorities (the Ethiopian Financial Intelligence Centre, the Regional and Federal Police, the National Bank).

6.3.7 Reporting

The compliance function shall document the work it has carried out to trace the interventions, as well as the recommendations made, risk of penalties, the remedial actions decided accordingly and other actions taken, in a quarterly report to the bank's senior management and the board. The report shall include:

a) an assessment of the risks of non-compliance and compliance by establishing the standards it has set in this regard;
b) information relating to the main problems noted, including the major business units and authorities contributing to the non-compliance and also the penalties and other administrative actions levied on the bank;
c) the list of alerts received through the exercise of employee whistle blowing procedure provided for under Sub-Article 6.3.10 of this Directive. This list shall be submitted to the National Bank;
d) description of the corrective measures undertaken and the reforms of the processes implemented, if applicable

6.3.8 New Products Policy

a) The compliance control function shall issue an opinion to any launch of a new product, new activity, any substantial change in the marketing policy of a product line or any entry into a new market. Exceptional asset acquisition or disposal operations shall also be the subject of a prior opinion from the compliance function.

b) If a negative compliance opinion is not taken into account, the compliance officer shall inform the senior management, or even the board directly. Mention of this opinion and the follow-up given shall be made in the quarterly report provided for in this Directive.

6.3.9 Control of the Compliance Function

The activities of the compliance function shall be subject to internal audit.

6.3.10 Whistle Blowing Procedure

a) A bank shall establish an employee warning procedure right to the compliance officer.

b) This procedure is intended to report violations of the law or regulations committed by the bank, when information by the usual reporting line is ineffective or impossible.

c) This procedure shall provide for the anonymity of the agents who initiated the alerts. It shall also provide that the author of an alert issued in good faith and in accordance with the conditions provided above cannot be sanctioned or incur harmful measures.

d) This procedure shall be established in accordance with the relevant National Bank Directive.

7. Third Line of Defense Control

7.1 General Principle

7.1.1 A bank's internal audit function constitutes the third line of defense in the system of internal control. It shall provide an independent assurance to the board and senior management on the quality and effectiveness of the bank's internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organization and its reputation.

7.1.2 The internal audit, which shall be performed independently, aims to verify compliance of operations, assess the risks incurred, the adherence to procedures and regulation, the efficiency and the appropriateness of the mechanisms for monitoring and the risk management, as well as other matters related to the activity of the bank and its subsidiaries, in accordance with the relevant National Bank Directives.

7.1.3 The internal audit function shall have a clear mandate, be accountable to the board and be independent of the audited activities. It shall have sufficient standing, skills, resources and

authority within the bank to enable the auditors to carry out their assignments effectively and objectively.

7.2 Responsibilities of Internal Audit Function

7.2.1 A bank's internal audit function shall carry out periodic checks of all activities conducted by the bank. To this end, in particular, the internal audit:

a) proposes an annual or multi-year audit plan, approved by the audit committee, and the allocation of its resources accordingly;
b) relies for the performance of its activities on a rigorous methodology to identify the significant risks incurred by the bank;
c) has sufficient resources experience to understand and evaluate the activities to be audited;
d) is kept informed in a timely manner of any material changes made to the bank's risk management strategy, policies or processes;
e) may communicate with any member of staff and has full access to records, files or data of the bank and its affiliates, whenever relevant to the performance of its duties;
f) has the authority to assess any outsourced functions;
g) formalizes and returns the conclusions of each of its activities in a written report, which is the subject of a contradictory discussion with the auditees, and which shall be sent promptly to the audit committee and to the senior management;
h) makes recommendations to ensure the effective implementation by structured monitoring procedures; and
i) access, for the purposes of its tasks, archives, files and data and any useful and necessary information, without restriction and in any form whatsoever.

7.2.2 Where a bank belongs to a bank group, the bank's internal auditors shall have access to any information that is useful and necessary for the performance of their tasks, regardless of the place in which this information is located. The framework to ensure this availability of information shall be part of the memorandum of association of the subsidiary in Ethiopia.

7.3 Audit of Other Control Functions

7.3.1 Internal audit shall be responsible for periodically evaluating the effectiveness of risk management and governance processes,

internal procedures and policies, as well as the proper functioning of the other lines of defense.

7.3.2 Internal audit shall also assess, and in a non-limiting manner:

a) the financial communication process, as well as the reliability and accuracy of the information communicated to the National Bank and to third parties;
b) the risk measurement and monitoring systems implemented by the second line of defense;
c) the internal procedures for assessing the adequacy of the bank's capital;
d) the procedures for managing business continuity within the bank; and
e) the controls carried out by the risk management department, by the compliance function and by the IT security function.

7.4 Reporting

7.4.1 Internal audit shall functionally report to the audit committee, and shall be established and shall function in accordance with the relevant National Bank Directive.

7.4.2 The head of internal audit shall report on the performance of his duties to the audit committee, and administratively to senior management and the board.

7.4.3 The head of internal audit shall inform, the audit committee and the board, of the shortcomings identified and of the recommendations formulated to strengthen the operational activities, the internal control and risk management systems and their implementation by the respective operational functions and risk management.

7.4.4 All the findings and recommendations shall be classified by order of risk magnitude or priority, with a classification of at least three (3) levels (high/medium/low).

7.4.5 The head of internal audit shall monitor the implementation of the corrective measures that are the subject of its recommendations and report on implementation status to the audit committee and to the board.

7.4.6 In the event of persistent non-execution of corrective measures decided in application of accepted recommendations contained

in an audit report, the head of internal audit shall inform, directly and on his own initiative, the audit committee and the board.

7.5 Coordination of Internal Audit with the Compliance Function

The head of internal audit shall also inform the head of compliance of any insufficiency observed relating to the management of the compliance risk and of any compliance incident.

8. Governance of Internal Control and Risk Management System

8.1 Role of the Board of Directors

8.1.1 Tasks

a) A bank's board of directors shall ensure that the bank's enterprise-wide risk management framework is commensurate with the complexity and risk profile of the bank. The board shall formally approve the components of the internal control and risk management framework:
   i. Risk strategy
   ii. Risk appetite
   iii. Risk management policies
   iv. Risk reports

b) The board shall ensure the adequacy of the three lines of defense system in relation to the risk appetite policy it has defined. The board shall also ensure implementation in an efficient manner, and that any deficiency or finding reported by the internal control functions is addressed in a timely manner by the senior management.

c) The board shall, on a quarterly basis, review the activity and results of internal control on the basis of the information sent to it by the internal audit function, by the chief risk officer, by the audit committee and, where applicable, by the senior management.

d) The board approves the overall internal control, compliance and risk management policy.

e) The board shall approve the operating charters of the audit committee and of any other committee.

f) The board shall receive information of any exchanges between the bank and the National Bank, and ensure execution of the requests from the National Bank.

g) If necessary, in addition to the reporting requirement provided in this

Directive, the board shall determine the nature, volume, form and frequency of the information transmitted to it.

h) The board shall approve all credit decisions concerning the large exposures. Prior to the review by the board, the risk management department shall issue an independent opinion on the large exposures

i) The board a shall approve related party transactions exceeding a specific amount or posing special, following internal audit's reasoned (non-binding) opinion to the audit committee, as provided for in the relevant National Bank Directives. The board may approve the transaction notwithstanding a negative opinion of the audit committee, provided the approval is fully disclosed to the National Bank, and the audit committee's opinion is submitted to it along with the disclosure report, as stipulated by the relevant National Bank Directive.

8.1.2 Delegation

The board shall clearly delineate the responsibilities of the members of the senior management and of the internal control and risk management functions and define the terms of the delegation's credentials.

8.1.3 Corporate Value

Members of the board and the senior management shall promote a strong culture of internal control, compliance and risk management that puts particular emphasis on the need, for each member of staff at all levels of the bank, to assume his duties in compliance with legal and regulatory provisions in force and the guidelines and the internal procedures. To this end, they adopt a training and information policy which highlights the bank's control objectives and explains the means of achieving them.

8.2 Role of Senior Management

8.2.1 Tasks

The effective implementation of the internal control, compliance and risk management system is the responsibility of a bank's senior management (CRO and CEO) which, in coordination, shall act as follows:

a) The CRO identifies all sources of internal and external risks; defines the appropriate internal control procedures; establishes the

appropriate organizational structure; and determines the human and material resources necessary for the implementation of the internal control system.

b) The CEO allocates resources (human, IT systems, logistical) to ensure, at all times, the overall proper functioning of the internal control, compliance and risk management system; and takes the necessary measures to remedy, in a timely manner, any deficiency or insufficiency identified.

c) In the event of disagreement on the necessary resources, the board shall make an arbitration after consulting the risk management and compliance committee, which may formulate proposals to the board to amend the organization of the internal control framework or to replace the heads of functions in case of deficiencies.

8.2.2 Information Sharing

The senior management (CEO and CRO) shall establish the procedures for exchanging information and documentation between the heads of the internal control and risk management functions and the operational departments.

9. Shari'ah Governance Framework

The Shariah governance framework shall be determined in line with the relevant National Bank Directive. It shall include the following three (3) governance bodies:

9.1 Shari'ah Committee

9.1.1 An interest-free bank (IFB)'s Shariah committee shall be responsible for the following:

a) ensuring that the bank's products and services are in compliance with Shari'ah principles;

b) review the bank's policies and procedures to ensure compliance with Shariah principles; and
c) consider and issue decisions, rulings and fatwas on all Shari'ah related issues faced by the business and operations of the IFB, whether it is referred to the Shariah committee or considered as part of its regular oversight responsibilities.

9.1.2 All decisions, rulings, fatwas of the Shariah committee shall always be binding on the IFB, whereas Shariah committee shall be responsible for all its decisions, rulings and fatwas.

9.2Shari'ah Compliance Function

The organization of an IFB's Shariah compliance function (SCF) shall fulfil the following characteristics:

9.2.1 the SCF shall report directly to the senior management of the IFB;

9.2.2 the SCF is subject to oversight of the board of the IFB as a control function, as well as oversight by the Sharia committee of the IFB in regard to compliance with the Sharia committee's rulings or fatwas;

9.2.3 the SCF shall coordinate the management of Shari'ah non-compliance risk faced by the IFB;

9.2.4 the SCF shall be independent of the operational units and shall be exclusive of the exercise of any other function within the IFB; and

9.2.5 the executive officer responsible for the management of SCF and the staff in charge of its operations shall have a high level of competence in the field of interest-free banking, Shari'ah rulings/fatwas and an in-depth knowledge of the related rules and standards; and

9.2.6 the SCF shall have dedicated and adequate staff of requisite competency and skills in managing IFB operations, consistent with the opinions and advice of the Sharia committee. The SCF shall have at least one qualified Shari'ah expert as a full-time staff member.

9.3Shari'ah Audit Function

An IFB shall put in place an independent Shari'ah audit function, as part of the IFB's internal control system. This audit function shall be responsible for, among other things, ensuring that all aspects of the IFB's business,

operations, products and services are in total compliance with Shari'ah principles.

10. Risk Management

10.1 General Provisions for Risk Management

10.1.1 Requirements for Risk Management

A bank shall fulfil the following risk management requirements:

a) establish a sound risk management culture throughout the bank;
b) manage the material risks of the bank's business activities;
c) identify fully, measure accurately, monitor frequently in order to prevent in a timely manner and minimize material risks;
d) control the risk position, ensuring compliance to the risk limits;
e) the risk-bearing decisions shall be clear, transparent and comply with risk management policies and risk limits; and
f) for interest-free banking activities, provide clarity on the role of Shari'ah committee to oversee that banks' products and activities comply with Shari'ah rules and principles. A bank with an interest-free window shall also ensure that it has the appropriate risk management policies and practices proportionate to its size, complexity, and nature of the operations, in accordance with the relevant National Bank Directive.

10.1.2 Proportionality

a) In accordance with Article 4.1.3 of this Directive, banks shall put in place a risk management policy proportionate to their size, complexity and business model.
b) When a bank is supervised on a consolidated basis, risk monitoring for the entire group shall be carried out by the parent company on a consolidated basis.
c) Banks shall ensure that the risk management is supported by:
    i. consistent and robust risk assessment approaches (i.e. quantitative and qualitative techniques) adapted to the bank's size, nature of business and complexity of activities;
    ii. adequacy and robustness of data;
    iii. appropriate measurement tools and methodologies; and
    iv. robust and sustainable measures for mitigating risks.
d) In any case, banks shall develop the following four components of the

risk management framework:

i. risk appetite statement, detailing the risk appetite and the risk tolerance accepted by the board, in the form of a statement revised and approved annually by the board;
ii. risk strategy revised and approved annually by the board;
iii. risk policies and procedures revised and approved periodically by the board, at least every two years; and
iv. risk reports submitted quarterly and annually to the board, formally endorsed by it, and sent for review to the National Bank.

10.2 Risk Appetite Statement

A bank's risk appetite statement (RAS) shall include the following components: risk mapping, risk indicators, risk tolerance statement and risk appetite decision.

10.2.1 Risk Mapping

a) A bank shall establish a risk mapping of its current activities, which shall meet the following characteristics:
   i. all inherent risks shall be listed comprehensively and be subject to an assessment;
   ii. risk mitigation mechanisms implemented shall be taken into account to reveal the residual risks; and
   iii. the level of sensitivity of the residual risks shall be assessed on a rating scale, according to a robust methodology approved by the board.
b) The result of the risk mapping shall be updated as necessary, at least once a year, validated by the CRO and by the senior management, approved by the board and distributed to the heads of the operational business lines and control functions.

10.2.2 Risk Indicators

a) The risk mapping shall take into account information on:
   macroeconomic and default indicators for credit risk, market risk and all relevant financial risks; and
   risk management incidents such as operational incidents, limit overruns or cash shortages, likely to impact the situation of the bank. This information, including record of the losses and near-losses, shall be kept in a database.

b) The board shall be informed of the risk indicators identified in the risk map.

10.2.3 Risk tolerance

a) A bank's risk tolerance represents the absolute limit that the bank may be exposed without jeopardizing the continuity of operations.
b) This limit shall be compatible with the bank's capital situation.
c) The risk tolerance shall be formalized in the RAS, and reviewed and approved at least once a year by the board or as needed, for example when the level of capital significantly changes.
d) Any operation or incident which would lead to crossing the risk tolerance thresholds defined by the bank's board shall be brought to the attention of the latter and the National Bank without any delay by the bank's CRO, with information to the board and senior management.

10.2.4 Risk Appetite

a) A bank's risk appetite is the level of risk that the bank is willing to take to meet the expectations of the shareholders in terms of profitability, gearing, security and sustainability. The risk appetite shall be inferior to risk tolerance.
b) When the residual risk level resulting from the risk mapping is considered excessive or is not consistent with the risk appetite approved by the board, additional risk mitigation measures shall be taken. If no additional mitigation, the risk appetite shall be modified accordingly and approved by a new decision of the board.

10.2.5 Indicators to include in the RAS

A bank's RAS shall provide, on the one hand, quantitative criteria expressed as a function of income, level of capital, risk indicators, liquidity and any other relevant parameter and, on the other hand, qualitative guidelines concerning risks, including reputation and ethics risks, as well as risks linked to combating money laundering and terrorism. The RAS shall include at a minimum:

a) the capital adequacy ratio (or CAR) target;
b) income criteria: Return on Equity (ROE) or/and Risk-Adjusted Return on Capital (RAROC) targets;
c) assets quality criteria: non-performing loans ratio, provisioning
d) liquidity criteria: reserve requirements, liquid asset to net liability, loan

portfolio composition (short, medium, long-term loans); and

e) other criteria determined by the board in accordance with this Sub-Article 10.2.5.

10.2.6 Modification of the risk level

a) Any major change in a bank's risk exposure or any significant incident likely to affect the level of risk appetite and the compliance with prudential regulations shall be brought immediately to the knowledge of the National Bank by the CRO, with information to the board.

b) The board shall be informed and meet without any delay to decide on corrective measures.

10.3 Risk Strategy

A banks' risk strategy is the set of rules adopted annually by the board to execute the risk appetite and meet shareholders' expectations. It reflects, for each type of risk and exposure, the instruments, limits, maximum loss and other relevant parameters that are authorized to the operational departments and that the risk management function shall identify, measure, monitor and control.

10.3.1 Credit risk strategy

a) A bank's credit risk strategy shall include a list of all types of applicable and approved transactions and financings. The approved list shall be kept up to date and communicated to the relevant personnel within banks, and an internal compliance function shall be organized and empowered to ensure that such rules are applied.

b) A bank's board shall annually approve the bank's credit risk strategy, which articulates the bank's overall direction for its credit activities. The board shall define and set its overall levels of risk appetite, risk diversification and asset allocation strategies applicable to each financing instrument (non-interest-free or interest-free), economic activity, geographical areas, season, currency, collateral and tenor.

c) A bank shall have adequate strategies to establish thresholds for acceptable concentrations of credit risk, reflecting the bank's risk appetite, risk profile and capital strength. For this purpose, all material concentrations shall be regularly reviewed and reported to the bank's board.

10.3.2 Market Risk Strategy

a) A bank shall develop a market risk strategy including the list of

allowable instruments, the level of acceptable market risk appetite taking into account contractual agreements with fund providers, types of risk-taking activities and target markets in order to maximize returns while keeping exposures at or below the pre-determined levels.

b) The market strategy shall be reviewed periodically by the board and at least annually, communicated to relevant staff, and disclosed to fund providers if any.
c) The market risk strategy shall include, at least:
    i. list of authorized instruments;
    ii. modalities for the computation of the risk position in the trading book;
    iii. principles of market risk management in normal conditions and in case of stress; and
    iv. principles of implementing market risk mitigating measures (detailed instruments and competence to approve them).
d) A bank market risk limits shall include, at least limits for:
    i. transacted product portfolio, transactors, limits, total risk position in the accounting book;
    ii. positive and negative foreign exchange position limit, transactors and loss; and
    iii. commodity price risk: limit for transacted product portfolios, transactors and loss limit.
e) Where a bank has a material trading portfolio (exceeding 5 percent of total assets), the bank shall set limits, including operational limits for trading desks, traders, products, instruments, markets, industries and regions. The limits shall be clearly understood, and any changes shall be clearly communicated to all relevant parties.
f) Risk-taking units shall remain within the set and approved limits at all times. Limit breaches shall be made known to appropriate senior management without delay. There shall be explicit policy as to how such breaches are to be reported to senior management and the actions to be taken.

10.3.3 Operational Risk Strategy

a) Operational risk management strategy of a bank shall include, at least the following elements:

i. principles of operational risk management, including identification and record keeping of operational risks, operational losses and near-losses;
ii. principles of outsourcing, insurance purchasing and technology application; and
iii. business continuity plans, including at least, loss of important documents and database; breakdown of the information technology system and cybersecurity risk; and force majeure (war, flooding, fire, etc.)

b) The operational risk limits include:
i. financial loss limit; and
ii. non-financial loss limits (also including prestige, reputation, legal obligations)

10.3.4 Liquidity Risk Strategy

a) A bank's liquidity risk strategy shall fulfil at least the following requirements:
i. maintain sufficient high-liquid assets in order to meet the bank's liquidity needs in both business-as-usual and liquidity stress scenarios (also including determination of losses and costs of meeting liquidity in the market);
ii. ability to determine the costs of meeting liquidity needs and liquidity risk in internal capital pricing,
iii. assessing results of the liquidity management on all material business activities (applied to both on- and off-balance sheet items);
iv. strategies to diversify sources and terms of mobilized capital in order to increase stability of liabilities and support daily liquidity; and
v. principles of liquidity stress test.

b) The liquidity risk strategy shall include limits, at a minimum, on the following parameters:
i. risk limits for ensuring a safe level of compliance to liquidity ratio, loan-to-deposit ratio, medium and long-term financing on short-term capital ratio, and other prudential ratios resulting from the National Bank prudential regulations; and
ii. other limits specified in the internal policies of the bank, in accordance with the risk appetite.

10.3.5 Concentration Risk Strategy

a) A bank's concentration risk strategies shall include rules for:
    i. credit granting;
    ii. proprietary transactions; and
    iii. funding concentrations.
b) The concentration risk strategies shall include at least the following elements:
    i. In the case of credit granting: principles of determining credit concentration limits, sorted by credit product, customer, industry and economic sector; criteria for identifying a group of connected counterparties, in accordance with the relevant National Bank Directive; and principles of determining diversification effects and degree of interaction between credit products, industries and economic sector.
    ii. In the case of significant proprietary transactions (representing more than 10% of the bank's capital): principles of determining proprietary transaction -meaning, transactions conducted while using the capital of banks- concentration limits, sorted by transaction partner, transaction product and type of currency; and criteria for determining proprietary transaction portfolios in order to impose proprietary transaction concentration limits, ensuring diversification effect and measuring the degree of interaction as specified in the bank's policies.
    iii. With regards to the funding concentration, principles for: ensuring the diversification of the sources of funding; assessing on a continuous basis, through appropriate stress tests, the risk of withdrawal of funds by the main depositors and the consequence on the liquidity situation of the bank; and assessing, on a continuous basis, the level of competition on the market for the collection of large deposits, including the remuneration of large deposits proposed by the competitors.
c) A bank's concentration risk limits shall include at least:
    i. In the case of credit granting: credit limit for one customer, groups of connected counterparties or customer and affiliated person compared to the total loan balance; and credit concentration limits for credit products, industries and economic sectors, based on the ratios of those entities' financing (loan) balances to the total financing (loan) balance.

ii. In the case of proprietary transactions: transaction concentration limits for transaction partners, transaction products and types of currency based on the ratios of those entities' balances on the total proprietary transaction balance.

iii. With regards to funding concentration: regular reports to the senior management and to the board on, for instance, the top ten (10) large depositors and on the Herfindahl index of the deposit portfolio.

10.3.6 Interest Rate Risk in the Banking Book (IRRBB) Strategy

A bank's IRRBB strategy shall include, at least the following elements:

a) principles of IRRBB management, which employ at least the following indices:
   i. repricing gap profile: the difference between the values of interest-bearing financial assets and interest-bearing financial liabilities at the time of new interest rate or repricing; and
   ii. the following indices to measure the influence of change in interest rate in pre-defined scenarios adapted to the bank's situation: change in Net Interest Income: caused by change in interest rates of financial assets and liabilities, as well as interest-bearing off-balance sheet items; and change in Economic Value of Equity: change in net value of income from financial assets and expense from financial liabilities when change in interest rate occurs.
b) principles of using the IRRBB prevention tools (including competence to approve those tools).
c) IRRBB risk limits shall include at least:
   i. the limit on difference between the values of main interest-bearing financial assets and main interest-bearing financial liabilities with the same time of new interest rate or repricing; and
   ii. the limit on change in net interest income and change in economic value of equity caused by change in interest rate according to the IRRBB management strategies.

10.3.7 Shariah-related risks Strategies

A bank having an activity made partially or total of interest-free banking shall define strategies for all Shariah-related risks, including rate of return risk, equity investment risk and other Shariah non-compliance risks, in accordance with the relevant National Bank Directive.

10.4 Risk Policies

10.4.1 General Principles

a) The risk management policies of a bank shall be formalized by the bank in the form of a set of procedures addressing all the risks identified in the risk appetite and risk strategies. The policies shall be prepared by the CRO, approved by the board and endorsed by the senior management. The board shall specify the procedures of the risk management function, roles and responsibilities and the exchange of information between the various stakeholders.

b) The risk management policies shall provide that the risk areas identified as the most sensitive are subject to reinforced management and monitoring and control measures.

c) The risk policies shall include, but not limited to the following:

   i. a description of the bank's risk management objectives and procedures by risk category or in aggregate;
   ii. structure and organization supporting the relevant risk management framework and functions;
   iii. scope and nature of the risk measurement and reporting system;
   iv. practices for mitigating risks, including monitoring the continuing effectiveness of risk mitigants.
   v. practices for creation, promulgation and imposition of risk limit for each type of material risk (also including risk limit creation methods, the individuals and divisions tasked with risk limit creation, risk limit allocation and actions against risk limit violations) and for each level of responsibility;
   vi. risk identification, measurement, monitoring and control for each type of material risk (also including risk measurement/control methods and models);
   vii. stress test;
   viii. mechanism for internal reports on risk management;
   ix. risk management for new products/operations in new markets; and
   x. other necessary contents according to CRO, board and senior management requirements for each type of material risk.

d) A bank's policies on risk management shall apply the following

principles:

i. the policies shall be appropriate for the business strategies, control culture, human resources, information technology infrastructure and management information system of the bank; and
ii. the risk positions and risk management violations shall be reported sufficiently and punctually to the board, to the CRO and to the senior management; there shall be a mechanism for taking action against risk management violations.

e) The risk management policies shall fulfil the following requirements:
   i. are properly documented;
   ii. created for between 3 and 5 years of application, undergoes both scheduled (at least once per year) and unscheduled assessment as specified by the bank to make timely adjustments in case of changes in the business and legal environment in order to fulfil risk management goals;
   iii. suitable for the interests of a bank's shareholders;
   iv. suitable for the capital level and the existing levels of its sources;
   v. have inheritance and continuity in order to ensure feasibility through the economic cycles; and
   vi. consistent with the risk management strategy and the established risk appetite.

f) A bank's risk policies, procedures and limits shall, inter alia:
   i. provide for adequate and timely identification, measurement, monitoring, control and mitigation of the risks posed by its financing, investing, trading, Shari'ah-compliant activities, off-balance sheet, fiduciary and other significant activities at the business line and bank-wide levels;
   ii. clearly delineate accountability, lines of control and lines of authority across the bank's various business activities, and ensure there is a clear separation between business lines and the risk function; and
   iii. include a schedule and process for reviewing the policies, procedures and limits, and for updating them as appropriate.

10.4.2 Risk Limits

a) A bank's risk policies shall include a risk limit framework for each risk considered in the risk strategy as stated under Sub-Article 10.3of this Directive.

b) The limits shall be issued and amended on the proposal of the CRO, in coordination with the senior management, and approved by the board. In the case of a foreign bank branch, the competence to promulgate and amend foreign bank branch's risk limit shall comply with the foreign parent bank's policies.
c) The risk limit framework shall be reviewed and re-assessed (adjusted if necessary) at least once per year or when a major change affects the risk position, as specified in the bank's own policies.

10.4.3 Risk Management for new Products and Operations in new Markets

a) A bank's risk management policies for new products/operations in new markets (within permitted business activities) shall fulfil the following requirements:
    i. criteria for determination of new products/operations in existing markets, and new products/operations in new markets; and
    ii. process for implementation of new products/operations in new markets, applying the following principles: the board approves policies on implementation of new products/operations in new markets, based on the senior management's proposal. The management approves plans for implementation of new products/operations in new markets; and in the case of a foreign bank branch, approval of policies on and plans for implementation of new products/operations in new markets shall be done as specified in the foreign parent bank's policies.
b) A bank's plan for implementation of new products/operations in new markets shall be appraised by the risk management function and by the compliance control function on risks, risk management measures and shall have at least cover the following:
    i. the scale and trial period of implementation of new products/operations in new markets shall be approved by the board, based on assessment of risks coming from those activities, as well as the way they may affect equity and income, in order to ensure their suitability for the bank's risk management capabilities; and
    ii. the official time for implementation of new products/operations in new markets shall be based on the trial

results compared with the risk management criteria of the bank.

c) When the implementation of new products/operations in new markets become effective, a bank shall promulgate new policies and carry out effective risk management for those activities.

10.4.4 Risk Identification, Measurement, Monitoring and Control

a) A bank's board shall be responsible for organizing the risk identification process in coordination with the CRO. The senior management shall be in charge of implementation of that risk identification process, in cooperation with the CRO. The outcome of this process shall be identification of all material risks and interaction of those risks.

b) A bank's risk management policies shall include the principles for risk measurement:
   i. a bank shall measure the risk level, based on determination of that risk's short-term and long-term effects on the bank's income, capital adequacy and business objectives achievement;
   ii. risk measurement shall be conducted using methods and models (also including the internal credit rating system) regularly assessed thoroughly for accuracy and appropriateness; and
   iii. risk measurement shall be carried out accurately and in a timely manner, in order to monitor and control risk effectively.

c) A bank's risk management policies shall include the principles for risk monitoring:
   i. a bank shall monitor its risk position, carry out timely assessments and give early warnings about the possibility of violations against risk limits and restrictions, in order to ensure operational safety; and
   ii. internal reports on risk monitoring shall be timely produced, accurate, complete and sent to related individuals and departments.

d) A bank's risk management policies shall include the principles for risk control:
   i. a bank shall control risk positions, transactions and activities according to their respective risk limits; and

ii. a bank shall have measures for prevention, minimization and timely handling risk to ensure compliance with limits and restrictions, operational safety, and have mechanisms for oversight and inspection of those measures' implementation.

e) A bank shall put in place management information systems (MIS) that allows analysis and measurement of all risks. The MIS shall be proportionate to the nature and volume of banks' operations. These MIS shall also make it possible to understand the analysis and measurement of risks in a transversal and prospective manner.

f) A bank's internal audit function shall be responsible for assessing on a periodic basis the suitability of the MIS to the current and future level, nature and criticality of risks.

10.4.5 Stress Tests

a) A bank shall conduct stress tests with the following parameters:
   i. Capital adequacy stress tests shall be conducted both on an annual basis and unscheduled (i.e. ad-hoc basis). A bank shall assess and demonstrate its ability to remain above the regulatory minimum capital requirements as prescribed by the National Bank, during a stress situation that is consistent with their stated risk appetite.
   ii. Liquidity stress tests shall be conducted both on a quarterly basis and unscheduled.

b) The stress test shall be conducted as follows:
   i. Sensitivity, scenario and reverse stress tests shall be performed.
   ii. For scenario stress tests, banks shall construct at least two scenarios (baseline scenario and adverse scenario). The chosen scenarios' likelihood shall be based on analyses of past events and macroeconomic forecasts.
   iii. A bank shall calculate the hypothetical effects on capital and liquidity ratios in each scenario.
   iv. A bank shall produce stress test reports (including quantitative data, as well as qualitative assessment and analyses) which shall be submitted to the board.

c) Based on the stress test results, a bank shall:
   i. assess the compliance with prudential and internal requirements;
   ii. formulate backup plans in case of failure to fulfil liquidity requirements; and

iii. calculate economic capital under the stress scenario to determine the capital target.

10.4.6 **Regular Review of Risk Policies**

a) A bank shall have a process for conducting regular independent reviews (i.e. independent assessment by internal and/or external auditors or third parties) of the soundness and the quality of its risk policies, in light of the bank's changing risk profile and the recent developments and changes in the bank's risk management.
b) A banks' risk policies shall be subjected to regular reviews by the National Bank against the expectations set out in this Directive.

10.5 Risk Reports

10.5.1 **Annual Risk Report**

a) A bank shall establish each year a Report on Governance and Risk Management.
b) The annual Report on Governance and Risk Management is intended to provide details on a bank's risk profile and on the management of the operational activities, support functions, governance arrangements and risks, with information/data as at 30 June of each fiscal year. The report shall be reviewed by the bank's internal audit function and approved by the board before being submitted to the National Bank.
c) The template for this report is determined annually by letter of the National Bank.

10.5.2 **Quarterly risk reports**

a) A bank shall establish quarterly a report on each material risk they bear in conducting their activities (see Sub-Article 6.2.7 of this Directive).
b) The template for this report is determined quarterly by letter of the National Bank.

11. Additional Requirements for Specific Risks

In addition to the general requirements on Risk Appetite Statement, Risk strategy, Risk policies and Risk reports, a bank shall put in place specific risk management features for each of the risks discussed below.

11.1 Credit Risk Management

As provided for under the relevant National Bank Directive, the

responsibility of credit risk management is vested in the board's credit committee, which shall ensure that the bank's credit risk profile is in line with the bank's risk appetite as defined by the board.

11.1.1 Credit Risk Framework and Oversight

a) A bank's framework for credit risk management shall include identification, measurement, monitoring, reporting and control of credit risks at a solo and consolidated basis, and the bank shall hold adequate capital against assumed credit risks.

b) A bank shall also comply with relevant rules, regulations and prudential conditions as set out by the National Bank applicable to the bank's financing activities. The bank's framework shall be consistent with the risk appetite, risk profile, systemic importance and capital strength of the bank, which shall take into account market and macroeconomic conditions, and result in prudent standards of credit underwriting, evaluation, administration and monitoring.

c) In addition to the general principles, a bank's board-approved credit policy and procedures shall establish an appropriate and properly controlled credit risk environment, which shall include, but not limited to:

   i. well documented and effectively implemented strategy and sound policies and processes for assuming credit risk, without undue reliance on external credit assessments;

   ii. well defined criteria and policies and processes for: approving new exposures (including prudent underwriting standards), and ensuring a thorough understanding of the risk profile and characteristics of the borrowers (and in the case of securitization exposures all features of securitization transactions) that would materially impact the performance of these exposures; renewing and refinancing existing exposures; and identifying the appropriate approval authority for the size and complexity of the exposures.

   iii. effective credit administration policies and processes, including: continued analysis of a borrower's ability and willingness to make all payments associated with the contractual arrangements (including reviews of the performance of underlying assets, e.g. for securitization exposures or project finance); monitoring of documentation,

legal covenants, contractual requirements, collateral and other forms of credit risk mitigation; and an appropriate exposure grading or classification system;

iv. effective information systems for accurate and timely identification, aggregation and reporting of credit risk exposures to the bank's board and senior management on an ongoing basis;

v. prudent and appropriate credit limits consistent with the bank's risk appetite, risk profile and capital strength, which are understood by and regularly communicated to relevant staff;

vi. exception tracking and reporting processes that ensure prompt action at the appropriate level of the bank's senior management or board where necessary; and

vii. effective controls (including in respect of the quality, reliability and relevance of data and in respect of validation procedures) around the use of models to identify and measure credit risk and set limits.

d) The credit risk policy shall be periodically reviewed and updated by the CRO, in coordination with the senior management, to reflect changes to the credit risk strategy or a bank's wider operating environment, and then approved by the board.

e) A bank shall constitute a credit management committee (CMC), preferably comprising of officers responsible for credit risk within the risk management department, credit department and treasury and others as appropriate. In line with the relevant National Bank Directive, this committee shall report to the board's credit committee. The CMC shall also report to the banks' board risk management and compliance committee, which is empowered to oversee credit risk-taking activities and overall credit risk management function of a bank.

11.1.2 Due Diligence Process in Evaluating Counterparties

a) In evaluating credit counterparties, a bank shall:

i. carry out a due diligence review in respect of counterparties prior to deciding on the choice of an appropriate financing instrument;

ii. establish policies and procedures defining eligible counterparties including sovereign, financial institutions, corporate, related parties and retail/consumer. These shall

cover the nature of approved financings and types of appropriate financing instruments;

iii. obtain sufficient credit information (including from Credit Bureau) to permit a comprehensive assessment of the risk profile of a counterparty prior to the financing being granted;

iv. have policies and procedures to monitor the total indebtedness of obligors to which it extends credit and any risk factors that may result in default, including significant unhedged foreign exchange risk; and

v. have a policy for carrying out a due diligence process (e.g. Value at Risk, score cards, ratings (both external and internal), stress testing and sensitivity analysis, amongst others) in evaluating counterparties.

b) In a financing involving several related agreements, a bank shall be aware of the binding obligations arising in connection with credit risks associated with each agreement and with the underlying assets for each agreement.

11.1.3 Measuring and Reporting Credit Risk

For the purposes of measuring and reporting credit risk, a bank shall:

a) have in place appropriate methodologies for measuring and reporting the credit risk exposures arising under each financing instrument. It shall recognize that the measurement of credit risk is of vital importance in credit risk management and a number of qualitative and quantitative techniques to measure risk inherent in credit portfolio are evolving;

b) develop and implement appropriate risk measurement and reporting methodologies relevant to each financing instrument in respect of managing its counterparty risks, which may arise at different contract stages;

c) ensure that adequate systems and resources are available to implement this methodology; and

d) maintain capital against credit risk exposures arising from each financing instrument.

11.1.4 Credit Risk Mitigation and Management of Collateral

a) A bank shall have in place applicable credit risk mitigating techniques appropriate for each financing instrument. This shall include, but not limited to:

i. a methodology for setting mark-up rates, meaning price discount or add-ons according to the risk rating of the counterparties, where expected risks shall have been taken into account in the pricing decisions;
ii. permissible and enforceable collateral and guarantees;
iii. clear documentation as to whether or not purchase orders are cancellable; and
iv. clear procedures for taking account of governing laws for contracts relating to financing transactions.

b) A bank is expected to include in its processes, an on-going monitoring of quality and valuation of any collateral. The valuation of collateral reflects the net realizable value, taking into account prevailing market conditions.
c) A bank shall establish limits on the degree of reliance of collateral and guarantees and their enforceability if the counterparty defaults in payment. A bank shall also protect itself against legal impediments that may restrict the accessibility to collateral when it needs to enforce its rights in respect of a debt.
d) A bank shall formally agree with a counterparty at the time of signing the contract on the usage, redemption and utilization of collateral if the counterparty defaults in payment.
e) The management of collateral shall be conducted in compliance with the relevant National Bank Directive.

11.1.5 Management of Weak Counterparties

a) A bank shall have appropriate credit management systems and administrative procedures in place to undertake early remedial action in the case of financial distress of a counterparty or, in particular, for managing problematic credits, potential and defaulting counterparties consistent with the relevant National Bank's regulations.
b) This system shall be reviewed on a regular basis.
c) Management of weak counterparties shall include the following requirements:
i. specific regulations on criteria and methods of identifying weak counterparties and credit requiring attention, which shall include at least the credit stipulated in the relevant National Bank Directive and the credit classified as high risk in the internal policy of the bank;

ii. step up assessment of customers' solvency and ability to collect using appropriate legal procedures;
iii. measures for handling and restructuring credit requiring attention, as well as debt collection plans;
iv. step up debt monitoring, oversight and collection; and
v. responsibilities of individuals and departments related to nonperforming credit (if any) in order to implement appropriate measures.

d) Remedial actions by a bank shall include both administrative and financial measures:
   i. Administrative measures may, inter alia, include: negotiating and following-up pro-actively with the counterparty; setting an allowable timeframe for payment or to offer debt-rescheduling or restructuring arrangements (without an increase in the amount of the debt for Interest-free banks); using a debt-collection agency (when created in Ethiopia); and resorting to legal action, for collecting any outstanding dues from defaulters.
   ii. Financial measures may include, among others: imposing penalties in the case of deliberate procrastination; and establishing the enforceability of collateral or third-party guarantees.
e) A bank shall manage weak counterparties and credit requiring attention in order to implement handling measures in a timely manner.
f) A bank shall have adequate policies and procedures, and organizational resources for the early identification and management of problem assets and the maintenance of adequate provisions as per the relevant National Bank Directive.

11.1.6 Internal Credit Rating System

a) A bank shall have an internal credit rating system.
b) The internal credit rating system shall fulfil the following requirements:
   i. the rating system's criteria shall be quantified in order to assess the customer's creditworthiness (also including social and macroeconomic conditions, as well as business environment affecting the customer's solvency);

ii. there shall be database and data management methods for credit risk quantification as required;
iii. the internal credit system's results shall periodically be independently assessed;
iv. there shall be sufficient information on the internal credit rating system to be provided upon request of the internal audit department, independent auditing firms and other relevant authorities during the processes of internal audit, inspection, oversight and independent audit.
v. A bank shall use the internal credit rating system, as well as loss measurement methods and models for credit risk measurement.

11.1.7 Credit Risk Monitoring and Control

a) A bank shall monitor and control credit risk of each credit granted and the entire credit portfolio, and shall have handling measures in case of decline in credit quality, fulfilling at least the following requirements:
   i. monitor the credit classification results;
   ii. assess adequacy of provisions for credit losses as specified by the relevant National Bank Directive;
   iii. control the actual credit risk position to comply with credit granting limit and credit risk limit as specified in the National Bank requirements and the bank's own internal policies.
b) Credit risk monitoring and control policies shall at least include the following:
   i. roles and responsibilities of individuals and departments that monitor and control credit risk;
   ii. frequency of review, ensuring that each credit shall be reviewed at least annually regardless of the level of risk, and that the frequency shall be gradually increased in consideration of the level of risk and of the importance of the exposure. High risk loans, high amount loans and non-performing loans shall be reviewed with the highest frequency;
   iii. exposure classification, and use of provisions for credit losses;
   iv. assessment criteria and methods for determining the degree of credit quality decline; and
   v. early-warning mechanism for credit quality decline.

11.1.8 Credit Granting Appraisal

a) A bank shall conduct credit granting appraisal, which shall include at least have the following:
    i. appraisal of the ability of a customer to fulfil its obligations (e.g. checking with credit bureau and financial statements);
    ii. Identification of the customer's connected persons, the total balance of credit extended to the customer and his/her affiliates;
    iii. the appraisal shall be based on the customer's credit rating (or credit scoring, if available), also including ratings from other credit institutions;
    iv. a bank shall assess the adequacy, legal status and recallability of collateral, in the case of credit granting with collateral; and
    v. a bank shall appraise the ability to fulfil obligations and commitments of the guarantor in the case of credit granting with guarantee from a third party.
b) During appraisal, if any line of communication with customers other than the bank's is used, for example if the credit is granted through an agent or an intermediary, a bank shall inspect the line of communication's information quality and independence from the party receiving credit.

11.1.9 Approval of Credit Risk-Bearing Decisions

A bank shall approve risk-bearing decisions as follows:

a) the competence to approve credit risk-bearing decisions and cases requiring higher competence's approval shall be determined by quantitative and qualitative criteria;
b) in the case of approval by a committee, the approving committee shall have the record of approval or any equivalent, which clearly states the reason for approval or rejection and include the committee members' opinions either in the record or its appendix. The approval committee members shall be responsible for their decisions;
c) the CRO or representatives of the risk management function shall not be member of the committee, however, the opinion of the risk management function shall be taken in consideration in the credit decision process;
d) a delegation framework shall provide for the level of decision and for the situations where the decisions are submitted to the non-binding opinion of the risk management function;
e) the information provided for approval of credit risk-bearing decisions

shall be sufficient and appropriate for the scale and type of credit. The list of information to be used as basis for approval of credit risk-bearing decisions shall be determined by the risk management function in order to ensure the effectiveness of credit risk management; and

f) if the risk management function does not approve a proposal of credit decision, an escalation process shall be put in place for final decision by a higher level of delegation and ultimately by the board. Credit decisions adopted despite a negative opinion of the risk management shall be reported to the National Bank.

11.1.10 Credit Management

A bank shall fulfil the following requirements while conducting credit management:

a) putting in place specific policies and procedures on responsibilities and competence of individuals and departments in creation and retention of credit records, ensuring sufficient credit records as specified in the National Bank's requirements;
b) disbursement shall be appropriate for the foreseen use of funds and type of credit;
c) oversight on credit after disbursement shall apply the following principles:
    i. inspection of loan use and implementation of other terms of the customer's credit contract;
    ii. assessment of factors affecting the customer's solvency;
    iii. conducting collateral management;
    iv. monitoring the repayment schedule, remind customers of their obligation to repay by deadlines, notify the competent level in a timely manner when a customer has the risk of failure to repay or late repayment.
d) maintenance of credit records, information on solvency and repayment history of customers and other relevant information as specified in the National Bank's requirements.

11.1.11 Internal Credit Risk Reports

a) On either unscheduled or at least on a quarterly basis, a bank shall produce internal credit risk reports.
b) The internal credit risk report shall include at least the following:
    i. quality of credit portfolios by customer, industry and economic sector;

ii. credit requiring attention and measures for handling them;
iii. customers, businesses and economic sectors having outstanding loan balances exceeding credit risk limits;
iv. value of collateral and collateral portfolios by type;
v. the state of establishment and use of provisions for credit losses;
vi. early warning about violations of credit risk limits and restrictions;
vii. violations in credit risk management and their causes;
viii. proposals and requests about credit risk management and the organizational levels they are submitted to; and
ix. the state of fulfilment of requests from internal audit, the National Bank, external auditors and other relevant authorities on credit risk management.

11.2 Market Risk Management

11.2.1 Market Risk Framework and Oversight

a) A bank shall have in place an appropriate framework for market risk management, including reporting, in respect of all assets held, even those that are not exposed to significant price volatility, whenever the bank's assets held for trading represent, for example, more than 5 % of its total assets or when its foreign net open position represents more than 10% of its capital, or similar internal limits which are more conservative than related market risk prudential limits stipulated in the relevant National Bank Directive.
b) A bank shall establish a sound and comprehensive market risk management process and information system, which, among others, shall comprise:
   i. a conceptual framework to assist in identifying underlying market risks;
   ii. effective information systems for accurate and timely identification, aggregation, monitoring and reporting of market risk exposure to the bank's board, risk management function and senior management;
   iii. internal systems and controls, and internal limits taking into account contractual agreements with fund providers in respect of all assets held, including those that do not have an active market and/or are exposed to high price volatility;

iv. guidelines governing risk-taking activities in different portfolios and their market risk limits;
v. appropriate market risk limits consistent with a bank's risk appetite, risk profile and capital strength, and with the management's ability to manage market risk and which are understood by, and regularly communicated to relevant staff;
vi. effective controls around the use of models, if applicable, to identify and measure market risk, and set limits;
vii. appropriate frameworks for pricing, valuation and income recognition; and
viii. a strong management information system for controlling, monitoring and reporting market risk exposure and performance to appropriate levels of senior management.

11.2.2 Market Risk Measurement, Monitoring and Control

a) A bank shall measure, monitor and control market risk as follows:
   i. the bank's units responsible for measuring, monitoring and controlling market risk shall be independent from the unit conducting the market transactions;
   ii. the bank shall ensure information technology infrastructure and database for market risk measurement, monitoring and control; and
   iii. specific competence shall be allocated to approve and implement market risk prevention measures.
b) A bank's method and model for measurement and monitoring of market risks based on interest rate, exchange rate, equity price and commodity price risks shall fulfil the following requirements:
   i. measure and monitor the market risk position associated with each financial asset, liability and off-balance item; and
   ii. parameters and assumptions shall be reviewed and adjusted, based on comparisons between the result of the method/model and actual events.
c) Market risk control shall fulfil the following conditions:
   i. provide early warnings about probability of violation against market risk limits; and
   ii. at the end of each transaction date, banks shall assess the compliance to market risk limits, based on the actual market risk position, as well as hedging transactions, where applicable.

11.2.3 Valuation and Model Validation

a) A bank shall have robust systems and controls, with documented policies and procedures for the valuation process.
b) The valuation policies and procedures shall, among others, include:
    i. clearly defined responsibilities of the personnel and departments involved in the valuation;
    ii. sources of market information, and review of their reliability;
    iii. frequency of independent valuations;
    iv. timing of closing prices;
    v. procedures for adjusting valuations between periods;
    vi. ad-hoc verification procedures; and
    vii. reporting lines for the valuation department that shall be independent from the front office.

11.2.4 Internal Market Risk Reports

a) By the end of each working day, a bank shall produce a daily report on market risk, including at least the following:
    i. the total risk position of the day;
    ii. actual and projected earnings or losses of proprietary transactions based on market prices; and
    iii. the day's transaction limits and the state of employing those limits until the end of transaction date.
b) On at least a quarterly basis, a bank shall produce internal market risk reports, which include, at a minimum, the following:
    i. the total market risk position compared to the market risk limit at the time the report is produced;
    ii. results of review and assessment of methods and models for market risk measurement and monitoring, as appropriate;
    iii. actual and projected earnings or losses of proprietary transactions based on market prices;
    iv. violations in market risk management and their causes, if any;
    v. extraordinary cases during proprietary transactions, changes to main assumptions of market risk measurement methods; and
    vi. the state of compliance with requests related to market risk management and proprietary activities from internal audit, the National Bank, external auditors and other relevant authorities.

11.3 Operational Risk Management

11.3.1 Operational Risk Framework and Oversight

a) A bank shall have in place a comprehensive and sound framework for

developing and implementing a prudent control environment for the management of operational risks arising from its activities.

b) The operational risk management framework shall be consistently implemented throughout the bank and understood by all relevant staff, and the controls shall provide reasonable assurance of the soundness of operations and reliability of reporting. Thus, a bank shall conduct periodic reviews to detect and address operational deficiencies. The reviews and evaluation of internal controls shall include independent audit coverage and assessment by internal and/or external auditors.

c) A bank shall ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to ensure that the inherent risks are well understood. A bank shall also ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

d) All operational losses and near-losses shall be recorded in an ad-hoc database. This database shall be reconciled periodically, at least quarterly, with the losses accounted in the bank's profit and loss account.

e) A bank shall implement a robust information technology risk management program in alignment with its operational risk management framework.

11.3.2 Operational Risk Identification, Measurement, Monitoring and Control

a) A bank shall fully identify operational risk in all of its products, business activities, business processes, information technology system and other management systems.

b) Operational risk identification shall be conducted for the following cases:

   i. internal fraud caused by swindling and misappropriating property, violation of strategies, internal policies and procedures related to at least one individual of the bank, as well as ultra vires acts, theft and abuse of internal information for personal gain;

   ii. external fraud caused by swindling and misappropriating property, committed by outsiders without assistance from or collusion with a bank's individual personnel and units, as well as

theft and forgery of bank cards and documents, breaking into the bank's information technology systems for theft of data and funds;

iii. involuntary violations related to customers, product provision processes and product properties while carrying out assigned customer-related functions and tasks within one's responsibilities, as well as violations against customer information security and anti-laundering regulations, and provision of products and service against regulations;

iv. damage to or loss of property, tools and equipment due to force majeure, human factor and other events;

v. interruption to business activities due disruptions of the information technology system, that is cybersecurity threat;

vi. limitations and drawbacks of transaction processes, control and management; and

vii. other cases specified in the internal policies of the bank.

c) A bank shall have operational risk measuring tools, using quantification of loss, and applying the following methods:

i. use audit findings, both internal and independent;

ii. collect and analyze internal and external loss data in order to determine loss, both internal and in the whole bank system;

iii. conduct operational risk control self-assessment in order to determine effectiveness of control activities for operational risk before and after control;

iv. employs business process mapping in order to determine operational risk level in each business process, the common operational risk of those processes and the interaction between those risks;

v. use risk and performance indicators to monitor factors affecting operational risk and identify latent limitations, problems and losses; and

vi. analyze scenarios in order to identify the sources of operational risk and set requirements for operational risk minimization and control in possible scenarios and events.

d) A bank shall conduct operational risk control through control activities, as well as other measures specified in the bank's internal policies. If the actual loss exceeds the operational risk limit as stated in the bank's risk appetite statement, the bank shall take

strengthening measures in order to control and minimize that operational risk in the future.

11.3.3 **Operational Risk Management for Outsourcing**

In accordance with the relevant National Bank Directive, a bank shall establish appropriate policies and processes to assess, manage and monitor the operational risks resulting from outsourced activities.

11.3.4 **Operational Risk Control and Mitigation including Insurance**

a) A bank shall put in place a strong control environment that utilizes policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.
b) The bank's internal control programmer shall include appropriate segregation of duties and consists of risk assessment, control activities, information and communication, and monitoring activities.
c) Where a bank's internal controls do not adequately address risk and exiting the risk is not a reasonable option, management may complement controls by seeking to transfer the risk to another party, such as through insurance.
d) A bank is, therefore, encouraged to purchase insurance for minimization of loss resulting from operational risk, suitable for the bank's financial capabilities and loss recovery. In this case, a bank shall assess the insurance provider's capability in executing insurance contracts.
e) A bank that does not purchase insurance for the aforementioned purpose shall assess the effectiveness of its minimization of losses resulting from operational risk.

11.3.5 **Operational Risk Stress Testing**

a) A bank shall conduct operational risk stress testing based on operational risk events which may be due to inadequate or failed internal processes, people and systems, including cyber events, or from external events, that may affect its products and activities.
b) A bank shall use its capital adequacy ratio as the main metric. A shall also consider the interactions of, and individual exposures to, idiosyncratic risk factors in determining its operational risk exposure, and analyze the possible interaction of operational risk losses with credit and market risks.
c) The analysis of the stress test events shall involve expert judgement, to include at least low-frequency high-severity events.

11.3.6 **Business Continuity Contingency Plans**

a) A bank shall prepare forward-looking business continuity plan with scenario analysis associated with relevant impact assessments and recovery procedures, to sustain its operations.
b) The business continuity contingency plan shall at least fulfil the following requirements:
    i. suitable for the bank's properties and operational scope;
    ii. include backup systems for human resources, information technology system and database;
    iii. have measures for minimizing loss coming from disruption;
    iv. be able to restore disrupted business activities back to the normal state within the requested time limit; and
    v. be reviewed and tested at least on an annual basis in order to determine the effectiveness of the plan to sustain operations and adjusted if necessary.

11.3.7 Internal Operational Risk Reports

a) A bank shall produce internal operational risk reports, either unscheduled or at least on a quarterly basis. Thus, reporting shall be timely and a bank shall be able to produce reports in both normal and stressed market conditions.
b) Reporting mechanisms shall be put in place at the board of directors, senior management, and business unit levels to support proactive management of operational risk.
c) A bank shall ensure that its reports are comprehensive, accurate, consistent and actionable across business units and products.
d) Reports shall be manageable in scope and volume by providing an outlook on a bank's operational risk profile and adherence to the operational risk appetite and tolerance statement.
e) The internal operational risk reports shall include at least contain the following:
    i. describe the operational risk profile of the bank by providing internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making;
    ii. breaches of the bank's risk appetite and tolerance statement, as well as thresholds, limits or qualitative requirements;
    iii. a discussion and assessment of key and emerging risks;
    iv. details of recent significant internal operational risk events and losses, including root cause analysis; and

v. relevant external events or regulatory changes and any potential impact on the bank.

f) Data capture and risk reporting processes should be analyzed periodically with the goal of enhancing risk management performance as well as advancing risk management policies, procedures and practices.

11.4 Liquidity Risk Management

11.4.1 Liquidity Risk Framework and Oversight

a) A bank shall establish a robust liquidity risk management framework that ensures it maintains sufficient liquidity, including a cushion of unencumbered, high quality liquid assets, to withstand a range of stress events, including those involving the loss or impairment of both unsecured and secured funding sources.

b) A bank shall manage its liquidity risk for:
   i. the bank's transactions, and where applicable, alongside its branches and other affiliates;
   ii. local currency and foreign currencies, including currencies with significant activity for the bank.

c) A bank's liquidity risk management shall include at least the following activities:
   i. manage liquidity within the day by monitoring that day's liquidity, identifying sources of capital, as well as the ability to mobilize those sources to maintain the day's liquidity, forecasting events that can drastically change such liquidity and propose handling measures;
   ii. manage high-liquid assets, based on market values, and their convertibility to cash for meeting liquidity requirements in both normal conditions and a low-liquidity market;
   iii. manage sources of mobilized capital by keeping statistics on the average demand deposit balance in a timespan of at least 30 days, core deposit balance and other indices for mobilized sources of capital as specified in the bank's internal policies;
   iv. manage the cash flow by creating a maturity ladder for the following day and specific timeframes (1 week, 1 month, 3 months, 6 months, 1 year and beyond 1 year) to determine the cash flow gap by comparing the inflows and outflows; and

v. manage liquidity sources by assessing those sources' accessibility in order to meet future liquidity needs in both normal conditions and a low-liquidity market condition.

d) A bank shall have in place a sound and comprehensive liquidity management framework, including reporting, taking into account separately and on an overall basis its liquidity exposures in respect of each category of current accounts, saving accounts, unrestricted and restricted investment accounts.

e) A bank's liquidity risk management process shall involve adequate tools to identify, measure, monitor, report and control the liquidity risk, including having a plan to meet contingency funding requirements and setting of limits on the basis of robust stress testing and scenario analysis.

f) With respect to liquidity risk management framework, a bank shall have an appropriate governance process, including board, chief risk officer (CRO) and senior management oversight, in order to identify, measure, monitor, report and control the liquidity risk.

g) A bank shall maintain adequate liquidity to always meet its obligations. In this regard, a bank shall have in place liquidity management policies, which shall be reviewed periodically, covering:
   i. a strategy for managing liquidity involving effective board, CRO and senior management oversight;
   ii. a framework for developing and implementing sound processes for measuring and monitoring liquidity;
   iii. adequate systems in place for monitoring and reporting liquidity exposures on a periodic basis;
   iv. adequate funding capacity, with particular reference to the willingness and ability of shareholders to provide additional capital when necessary;
   v. diversification in the sources, including counterparties, instruments, currencies and markets; and tenor of funding, and regular review of concentration limits; and
   vi. liquidity crisis management.

h) A bank's liquidity management policies shall incorporate both quantitative and qualitative factors:
   i. quantitative factors including the extent of diversity and sources of funds, concentration of the funding base, reliance on

marketable assets, or availability of standby lines of external funding; and

ii. qualitative factors including assessment of the general ability of the management, particular skills in treasury management and public relations, quality of management information system, a bank's reputation in the market, the willingness and ability of shareholders to provide additional capital and, in the case of a branch or subsidiary, the willingness and ability of the parent bank to provide liquidity.

11.4.2 **Liquidity Risk Identification, Measurement and Monitoring**

a) A bank shall ensure effective information systems to enable active identification, aggregation, monitoring and control of liquidity risk exposures and funding needs, including active management of collateral positions.

b) Liquidity risk identification shall fulfil the following requirements:
   i. analysis of liquidity needs, liquidity source of each business activity, asset-liability structure, on- and off-balance cash flows and liquidity's accessibility in the market; and
   ii. identification of liquidity risk coming from credit risk, market risk, operational risk, reputational risk, among other.

c) Measuring and monitoring liquidity shall at least fulfil the following requirements:
   i. appropriate tools are in place for liquidity measurement, which includes at least the following: future cash flows of both assets and liabilities; extraordinary liquidity needs and cases that require fulfilling off-balance obligations; transaction currency; and activities of the bank's agencies, deposits and payments.
   ii. appropriate tools shall be in place for monitoring the compliance with solvency and liquidity ratio, financing-to-deposit ratio, medium and long-term loan on short-term capital ratio and other liquidity ratios, if any.

d) A bank shall perform periodical cashflow analysis (gap analysis) under various market scenarios and conditions covering behavioral assumptions and contractual maturities. The analysis shall be based on relevant assumptions including factors affecting the bank's on- and off-balance sheet exposures. In this respect, a bank shall identify any future shortfalls in liquidity by constructing maturity ladders based on appropriate time bands. The bank shall consider

differentiating the types of cash flows as indicated below:

i. known cashflows – the maturities and the amounts are known in advance;
ii. conditional but predictable cashflows – conditionality is defined in terms of the type of contract or performance of work based on the agreed terms and conditions over an agreed period; and
iii. conditional and unpredictable cashflows.

11.4.3 Liquidity Risk Mitigation and Control

a) A bank shall maintain a cushion of unencumbered, high quality liquid assets to be held as insurance against a range of liquidity stress scenarios, including those that involve the loss or impairment of unsecured and typically available secured funding sources. In that regard the bank shall ensure that there no legal, regulatory or operational impediment to using these assets to obtain funding.
b) A bank shall assess the necessity and extent of its access to available funding sources. In managing its liquidity, a bank shall assess the following possible funding sources – natural cash flows arising from its usual banking activities, the realization of tradable invested assets, asset securitization, and its capacity to access shareholders' and/or where applicable, its bank group funds.
c) A bank shall actively manage its collateral positions, differentiating between encumbered and unencumbered assets, including monitoring the legal entity and physical location where collateral is held and how it may be mobilized in a timely manner.
d) A bank's liquidity management policies shall include some form of contractually agreed orderly liquidation procedures, to avoid having to liquidate assets at unfavorable prices, resulting in the erosion of the bank's capital and damage to the bank's reputation and viability. In this respect, a bank shall have a liquidity contingency plan addressing various stages of a liquidity crisis. A bank shall define the classification of these stages but may consider differentiating the stages as follows:
    i. identification of a liquidity gap or a situation which acts as a triggering event where withdrawals do not follow predictable patterns when, for example, banks may suffer an institutional rating downgrade;
    ii. need to liquidate assets or investments in an orderly manner to meet such a liquidity gap or situation; and

iii. emergency measures to be taken in the event that the previous steps fail to meet the liquidity gap adequately.

11.4.4 Liquidity Stress Tests

a) A bank shall conduct liquidity stress tests on a regular basis by applying various scenarios on its liquidity positions to ensure that it identifies sources of potential liquidity strain and have adequate liquidity to withstand stressed conditions.
b) While a bank is encouraged to cover stress events of different types and levels of adversity, it should include the following scenarios in their stress testing exercise:
    i. bank-specific crisis scenario, and where applicable, the stress testing should also incorporate bank group level scenarios; as well as
    ii. general market crisis scenario.
c) A bank shall have methods for calculating the impact of assumptions in order to assess the ability to fulfil obligations and commitments, as well as compliance to liquidity risk limits. Assumptions and methods for calculating the impact of assumptions on liquidity shall be reviewed and assessed for suitability.
d) The stress scenario shall have at least assumptions about deposits and credit quality, including interplay between deposits, credit quality and financing.
e) A bank's board of directors and senior management shall examine stress-testing results and adjust liquidity risk management strategies, policies, and positions to develop effective contingency plans, as well as formulate appropriate strategies to address the cash-flow needs reflected from the scenario analysis.

11.4.5 Contingency Liquidity Plan

a) A bank shall have a contingency liquidity plan that projects of future cashflows and funding sources of a bank under stressed market scenarios including aggressive asset growth or rapid liability erosion.
b) The plan shall be updated and reviewed on a periodic basis, at least annually, to ensure that it remains robust over time and reflects the bank's changing operating circumstances.
c) At a minimum, the contingency liquidity plan shall:
    i. designate the personnel responsible for the identification of crisis and for contingency management. This shall include

provisions for prompt notification of problems to the National Bank;

ii. specify the early warning indicators that are used to signal an approaching crisis event, and mechanisms to facilitate constant monitoring and reporting of these indicators;

iii. set out procedures for making up cashflow shortfalls in crisis situations, clearly stating sources of funds, their expected reliability and the priority ranking of the sources;

iv. outline courses of action for altering asset and liability structure and assess the likely impact of these on the market's perception of the bank; and

v. include details for handling public relations issues and media management.

11.4.6 Internal Liquidity Risk Reports

a) Either unscheduled or at least on a quarterly basis, a bank shall produce internal liquidity risk reports.

b) The internal liquidity risk report shall contain at least the following:

i. appraisal of the bank's credit rating, funding liquidity and the market's state of liquidity;

ii. appraisal of the liquidity governance process, including board and senior management oversight;

iii. the structure of the balance sheet; new capital-mobilizing products; depositors including investment accounts; deposit terms and profit rates;

iv. assessment of liquidity management policies including both qualitative and quantitative factors;

v. assessment of periodical cashflow analyses under various market scenarios and conditions ('normal' and 'adverse') covering behavioral assumptions and contractual maturities;

vi. liquidity sources, cash flow gaps, maximum amounts of cumulative liquidity mismatches, terms of capital, state of compliance with liquidity risk limits;

vii. results of liquidity stress tests in the reporting period;

viii. assessment of contractually agreed orderly liquidation procedures and liquidity contingency plan addressing various stages of a liquidity crisis;

ix. appraisal of the interactions between liquidity risk and other risks (e.g. market, credit, operational, displaced commercial risk,

and reputational and Shari'ah non-compliance risk) and interaction between the funding and market liquidity;

x. proposals and requests about liquidity risk management and the levels they are submitted to; and

xi. the state of fulfilment of requests from internal audit, the National Bank, independent auditing firms and other relevant authorities on liquidity risk management.

11.5 Concentration Risk Management

11.5.1 Concentration Risk Framework and Oversight

a) A bank shall put in place adequate policies and processes to identify, measure, evaluate, monitor, report and control or mitigate concentrations of risk on a timely basis. In this respect, a bank shall ensure that:

   i. it establishes thresholds for acceptable concentrations of risk, reflecting the bank's risk appetite, risk profile and capital strength, which are understood by, and regularly communicated to relevant staff; and

   ii. policies and processes are in place for all material concentrations to be regularly reviewed and reported to the bank's board.

b) A bank shall ensure that its management information systems identify and aggregate on a timely basis, and facilitate active management of, exposures, creating risk concentrations and large exposure to single counterparties or groups of connected counterparties.

c) A bank shall identify concentration risk at least in credit and proprietary transactions, including its on- and off-balance items.

d) A bank shall measure concentration risk based on assessment of each concentration risk-bearing credit and proprietary transaction's influence on income.

e) A bank shall control concentration risk as follows:

   i. monitor and check credit balance and proprietary transaction balance by concentration risk limits; provide early warning about balances and transactions that nearly exceed the concentration risk limits; and

   ii. implement measures for handling cases that exceed the concentration risk limits in a timely manner.

f) A bank shall include the impact of significant risk concentrations in its stress testing programmers for risk management purposes.

11.5.2 Internal Concentration Risk Reports

a) Either unscheduled or at least on a quarterly basis, a bank shall produce internal concentration risk reports.

b) The internal concentration risk report shall include at least the following:

   i. credit structure sorted by credit product, customer, industry and economic sector;

   ii. proprietary transaction portfolio structure sorted by transaction partner, customer, industry and economic sector;

   iii. the state of consumption concentration risk limits; reasons for exceeding such limits, if any;

   iv. proposals and requests about concentration risk management and the levels they are submitted to; and

   v. the state of fulfilment of requests from internal audit, the National Bank, external auditors about concentration risk management.

11.6 Management of Interest Rate Risk in the Banking Book

11.6.1 Interest Rate Risk in the Banking Book (IRRBB) Framework and Oversight

a) A bank shall identify, measure, monitor and control IRRBB in accordance with the following requirements:

   i. there are processes of IRRBB identification, measurement, monitoring and control, both unscheduled and scheduled (at least on a quarterly basis), as specified in the bank's internal policies.

   ii. The bank's units responsible for IRRBB identification, measurement, monitoring and control shall be independent from business units that generate IRRBB; and

   iii. there are information technology infrastructure and database in order to measure, monitor, control and produce internal reports on IRRBB.

b) The index for measuring the impact of interest rate changes shall include both of the following indices:

   i. change in Net Interest Income: Is the level of change in net interest income due to changes in interest rates from financial

assets, financial liabilities and interest-bearing off-balance sheet items in the banking book; and

ii. change in Economic Value of Equity: Is the level of change in the net present value of cash inflows of financial assets and cash outflows of liabilities when interest rates change.

11.6.2 Internal IRRBB Reports

a) Either unscheduled or at least on a quarterly basis, a bank shall produce internal IRRBB reports.

b) The internal IRRBB report shall include at least the following:

i. the interest rate gap, change in net interest income and change in economic value of equity, if available;

ii. the state of compliance with IRRBB limits;

iii. IRRBB prevention tools and the results of their implementation;

iv. proposals and requests about IRRBB management and the levels that the requests are submitted to; and

v. the state of fulfilment of requests from internal audit, the National Bank, external auditors about IRRBB management.

11.7 Other Risks

a) Depending on its situation, a bank may be exposed to other risks: reputational risk, strategic risk, insurance risk, business risk, pension risk, participation risk, funding cost risk, climate-related risk, model risk, etc.

b) It remains a bank's responsibility to determine all of its material risks, and all concentrations between and within those risks, irrespective of whether such risks are listed in this Directive or not. A bank shall also be responsible to determine the risk appetite, the risk strategy, the risk policies, including the framework to identify, measure, monitor and control these risks, and the reporting modalities.

12. Repeal

Bank Risk Management Guideline of 2010 is hereby repealed and replaced with this Directive.

13. Effective Date

This Directive shall enter into force as of ---- day of ----- 2025.