**BANK OF MAURITIUS**

# Guideline on Compliance Risk Management and Governance Framework

**November 2024**

*This page is intentionally left blank.*

## TABLE OF CONTENTS

*This page is intentionally left blank.*

# INTRODUCTION

## Background

The Guideline on Compliance Risk Management and Governance Framework draws on the guiding principles of the Basel Committee on Banking Supervision (BCBS) contained in its publication 'Compliance and the compliance function in banks' and on international best practices.

## Purpose

An effective management of compliance risk is key to ensure the safety and soundness of financial institutions.

The Guideline on Compliance Risk Management and Governance Framework ("Guideline") sets out the minimum requirements in order to assist financial institutions in implementing a strong compliance culture and an effective governance and risk management framework for compliance risk. Financial institutions are recommended to establish frameworks which are commensurate with the size, nature and complexity of their business operations.

Financial institutions should ensure that compliance forms part of the culture of the organisation and is not only the responsibility of compliance function staff.

## Authority

This Guideline is issued under the authority of section 50 of the Bank of Mauritius Act 2004 and section 100 of the Banking Act 2004.

## Scope of Application

This Guideline applies to all banks, non-bank deposit taking institutions and cash dealers licensed by the Bank of Mauritius.

## Effective Date

This Guideline shall come into effect on 12 November 2024.

## Interpretation

In this Guideline: -

**"Bank"** means the Bank of Mauritius established under section 3 of the Bank of Mauritius Act;

**"banking laws"** –

(a) means the Banking Act 2004, the Bank of Mauritius Act, the Convention for the Suppression of Financing of Terrorism Act, the Financial Crimes Commission Act 2023, the Financial Intelligence and Anti-Money Laundering Act, the Prevention of Terrorism Act, the Prevention of Terrorism (International Obligations) Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019; and

(b) includes such other enactment as may be prescribed;

**"board"** means the board of directors of a financial institution except for branches of foreign banks where "board" means the local advisory board/committee. For branches of foreign banks with no local advisory board, the responsibilities assigned to the board shall rest on the Chief Executive Officer of the branch;

**"compliance function"** refers to all staff carrying out compliance responsibilities. This includes the Head of Compliance and other staff in the compliance function within the second line of defence as well as, where applicable, other staff who have been assigned with compliance responsibilities. The compliance function, where relevant, may rely on the legal department of the financial institution;

**"compliance risk"** refers to the risk of legal or regulatory sanctions and other action, financial loss, damage to reputation or impairment of integrity or any other financial or non-financial impact that may arise due to non-compliance with legal, regulatory and other compliance obligations in Mauritius and in other jurisdictions where the financial institution is conducting its operations;

**"control functions"** mean those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance. This includes the risk management function, the compliance function and the internal audit function;

**"financial institution"** means any bank, non-bank deposit taking institution or cash dealer licensed by the Bank;

**"Head of Compliance"** means the senior officer in charge of the compliance function appointed under section 46(2) of the Banking Act;

**"legal, regulatory and other compliance obligations"** include

(a) banking laws and other laws as applicable, regulations, guidelines and other instructions issued by the Bank;
(b) laws, regulations, guidelines and other instructions issued by legislators and supervisors as applicable to the Financial Institution Group; and
(c) standards, market conventions, code of practice promoted by relevant industry associations; and

**"senior management''** constitutes a core group of high-level executives, including the CEO and other senior officers, with responsibility and accountability to the board for the sound and prudent day-to-day management of the financial institution.

## Section I – Governance Framework

### Compliance Policy

1.1 Financial institutions shall establish a comprehensive board approved policy on compliance risk management and governance framework (compliance policy), either on a stand-alone basis or integrated within relevant existing policies. The policy may be supplemented by other relevant documents. The policy shall be commensurate with the size, nature and complexity of the activities of the financial institution.

1.2 The policy and the relevant supporting documents shall clearly define, *inter alia*:

(a) the financial institution's expectations on compliance culture;

(b) the principles to be followed by all staff of the financial institution;

(c) the structure (including the broad categories of staff), the roles and responsibilities and reporting lines of the compliance function;

(d) the roles and responsibilities of other staff performing compliance responsibilities;

(e) the measures to ensure independence of the compliance function and avoid potential conflict of interest;

(f) the roles and responsibilities of business lines as the first line of defence, the risk management function and the internal audit function in providing independent assurance (as relevant) within the financial institution;

(g) the framework for identifying, documenting, assessing, monitoring, managing and reporting on compliance risk throughout the financial institution;

(h) the reporting requirements of the compliance function to senior management and the board or the designated sub-committee[1] of the board;

(i) the framework for assessing, resolving, escalating and reporting of compliance breaches and other related issues;

(j) the framework for determining disciplinary measures in case of non-compliance with the legal, regulatory and other compliance obligations, the compliance policy, processes and procedures and the internal codes of conduct;

(k) the training requirements;

(l) the relationship of the compliance function with other control functions;

(m) the succession plans for the Head of Compliance;

[1] As applicable under paragraph 1.6

(n) the right of access to the information and the right to conduct relevant investigations by the compliance function and the obligation of other staff to co-operate with the compliance function in supplying the information;

(o) the requirements for the compliance function to conduct investigation; and

(p) the rights of the compliance function in respect of hiring of external experts for the conduct of investigations, if appropriate.

**Compliance Culture**

1.3 Financial institutions that knowingly participate in transactions intended to be used by customers to avoid regulatory or financial reporting requirements, evade tax liabilities or facilitate illegal conduct shall be exposing themselves to significant compliance risk.

1.4 Financial institutions shall have a compliance culture which:

(a) starts with the tone from the top and where the board of directors and senior management serve as a model;

(b) places importance on high standards of honesty and integrity and promotes compliance with applicable legal, regulatory and other compliance obligations;

(c) regards compliance risk management as a fundamental element of the financial institution's business activities and involves each and every one within the organisation;

(d) ensures that compliance risk management is not only the responsibility of staff in the compliance function but of all business lines and staff such that all staff are responsible for managing compliance risk inherent in the day-to-day activities, processes and systems;

(e) maintains high standards and always endeavours to abide by the spirit as well as the letter of the law;

(f) is promoted through training/ awareness programmes and appropriate disciplinary measures for non-compliance; and

(g) is fostered through the establishment of an effective compliance function with appropriate stature, authority and independence.

**Responsibilities of the Board of Directors**

**Principle 1**

**The financial institution's board of directors is responsible for overseeing the management of the financial institution's compliance risk. The board should approve the financial institution's compliance policy, including a formal document establishing a permanent and effective compliance function and the corresponding responsibilities as well as the position of Head of Compliance. At least once a year, the board or a committee of the board should assess the extent to which the financial institution is managing its compliance risk effectively.**

1.5 The board shall:

(a) establish the compliance function and approve its structure, including the position of the Head of Compliance;

(b) set the tone from the top and promote the values of honesty and integrity and a strong compliance culture within the organisation;

(c) ensure that the financial institution has an appropriate policy and related processes, and procedures to identify, analyse, measure, mitigate, manage and monitor its compliance risk;

(d) review and approve the compliance policy annually;

(e) review the effectiveness of the compliance risk management and governance framework annually;

(f) ensure that it receives regular reports, at least on a quarterly basis, from the compliance function or the designated sub-committee[2];

(g) ensure that compliance issues are resolved effectively and promptly by senior management with the assistance of the compliance function and that appropriate measures including, where relevant, disciplinary actions are taken;

(h) review and approve the compliance programme annually;

(i) ensure that the compliance function and the Head of Compliance are given appropriate stature, authority and independence;

(j) ensure that the compliance function is provided adequate budgetary/financial resources to effectively discharge its responsibilities;

(k) approve the appointment, remuneration and termination of the Head of Compliance and review his/ her performance at least annually;

[2] As applicable under paragraph 1.6

(l) meet the Head of Compliance at least once every six months where senior management including the CEO shall not be present (this shall not be applicable to branches of foreign banks with/with no local advisory board); and

(m) meet the Head of Compliance at his/her request in addition to the semi-annual meetings, as required.

1.6 The board may, at its discretion, delegate the above roles and responsibilities (with the exception of the approval of the compliance policy, structure and appointment of Head of Compliance) to the Audit Committee or the Risk Management Committee of the board. In such instances, the Audit Committee or the Risk Management Committee of the board shall submit quarterly reports to the board on its proceedings and ensure that the board is promply apprised on material developments.

1.7 Compliance risk should be a standing item on the agenda of board meetings at least on a quarterly basis and be duly discussed at these meetings.

**Responsibilities of Senior Management**

**Principle 2**

**The financial institution's senior management shall be responsible for the effective management of the financial institution's compliance risk.**

**Principle 3**

**The financial institution's senior management shall be responsible for establishing and communicating a compliance policy, for ensuring that it is observed and kept up to date, and for reporting to the board of directors on the management of the financial institution's compliance risk.**

1.8 The senior management shall:

(a) be responsible for ensuring that the compliance policy is duly prepared, kept updated and approved by the board;

(b) ensure that all policies, procedures and processes are duly prepared and approved and kept updated;

(c) ensure compliance with the compliance policy;

(d) be responsible for prompt resolution of non-compliance issues;

(e) report to the board or the designated sub-committee[3] on an annual basis on the effectiveness of the financial institution's management of its compliance risk and governance framework in such a manner as to assist board members to make an

[3] As applicable under paragraph 1.6

informed judgment on whether the financial institution is managing its compliance risk effectively;

(f) report promptly to the board or the designated sub-committee[4] on any material compliance failures (e.g. failures that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation);

(g) ensure that the compliance policy, procedures and processes are communicated to all staff and observed at all levels of the financial institution;

(h) identify and assess, with the assistance of the compliance function, at least once a year, using a Risk Based Approach, the compliance risks facing the financial institution, the shortfalls in terms of policy, procedures, implementation or execution and the risk mitigating plan;

(i) ensure that compliance risk assessments are promptly conducted and updated when there are material developments and incidents; and

(j) have an ongoing oversight on the continued compliance by the financial institution with all the applicable legal, regulatory and other compliance requirements, with the assistance of the compliance function.

**Principle 4**

**The financial institution's senior management is responsible for establishing a permanent and effective compliance function within the financial institution as part of its compliance policy.**

1.9 The senior management shall:

(a) ensure that the financial institution has in place a reliable, permanent, independent and effective compliance function commensurate with its size, nature of operations and complexity;

(b) ensure that the Head of Compliance and other staff in the compliance function are not placed in a position of conflict of interest between their compliance responsibilities and other responsibilities;

(c) ensure that the remuneration of the Head of Compliance and other staff in the compliance function do not pose any conflict of interest;

(d) provide sufficient resources for the compliance function, including competent and experienced officers, and budget;

(e) ensure that the compliance function has the required right of access to information and the right to conduct relevant investigations;

[4] As applicable under paragraph 1.6

(f) ensure that the compliance function has access to relevant personnel/ management for performing its role;

(g) ensure that the compliance function can have recourse to internal/external expertise in specific areas where required;

(h) ensure that the compliance function is kept informed of changes in the activities and strategy of the financial institution and on any other incidents/ issues related to compliance for the timely identification of compliance risk;

(i) ensure that sufficient and ongoing training is provided to the staff in the compliance function and other staff to keep them equipped and be abreast of developments on applicable legal, regulatory and other compliance obligations; and

(j) promptly inform the board and the Bank if the Head of Compliance resigns and provide the reasons for the resignation as well as any changes thereof.

## Section II – Compliance Function

### Compliance Function Principles

### Principle 5: Independence

**The financial institution's compliance function should be independent.**

2.1 The compliance function shall:

(a) be headed by a Head of Compliance;

(b) be in the second line of defence and independent from business lines to avoid any undue influence or conflict of interest;

(c) have a formal status within the financial institution with an appropriate standing, authority and independence;

(d) report directly to the board or the designated sub-committee[5];

(e) submit regular reports, at least on a quarterly basis, to the board or the designated sub-committee[5], but any material compliance failure should be reported immediately;

(f) ensure that staff with compliance responsibilities residing in other business units do not have any conflict of interest between their compliance responsibilities and any other responsibilities they may have and have a reporting line to the Head of Compliance;

(g) have the right on its own initiative to have access to any staff member and to any information required to fulfil its responsibilities; and

(h) have the right to carry out investigations and to seek assistance from internal and external specialists as deemed relevant in this respect.

### Head of Compliance

2.2 The Head of Compliance shall:

(a) be a senior officer as set out in the Guidelines on Section 46(2) of the Banking Act 2004 - Appointment or Reappointment of Senior Officers;

(b) have a good knowledge of compliance risks to which the financial institution is exposed and its legal, regulatory and other compliance obligations;

(c) be supported by sufficient resources, including competent officers and budgetary resources, to carry out assigned responsibilities effectively;

[5] As applicable under paragraph 1.6

(d) be responsible for co-ordinating the identification and management of the compliance risk and for supervising the activities of all staff in the compliance function;

(e) not have direct business line responsibilities or other responsibilities which could pose a conflict of interest;

(f) keep the Chief Risk Officer well informed of compliance risk-related issues so that the latter can address risks at an Enterprise-Wide level;

(g) have the overall authority and responsibilities for reporting to the board or the designated sub-committee[6] and for engaging effectively with senior management; and

(h) have direct access to the board or the designated sub-committee[6] and be given the opportunity to discuss issues faced by the compliance function regularly with the board or the designated sub-committee[6].

**Conflicts of Interest**

2.3 The Head of Compliance and other staff of the compliance function should not be entrusted with and/or be engaged in any other responsibilities nor be a member of any committee which could result in real or possible conflicts of interest. In case the Head of Compliance or other staff of the compliance function is a member of such committee, their role shall only be an advisory one with no voting power.

2.4 The remuneration of the Head of Compliance and other staff in the compliance function shall be mainly based on the achievement of their compliance function responsibilities and shall not be linked in any way to the financial performance of any business line/function.

**Compliance Function Resources**

**Principle 6: Resources**

**The financial institution's compliance function should have the resources to carry out its responsibilities effectively.**

2.5 The compliance function shall:

(a) be sufficiently staffed with appropriate resources commensurate with the size, nature and complexity of the financial institution to ensure that its responsibilities are discharged effectively;

[6] As applicable under paragraph 1.6

(b) comprise of staff with the required qualifications and experience who understand the legal, regulatory and other compliance obligations applicable in Mauritius and in other jurisdictions where the financial institution is conducting its operations and their impact on the financial institution;

(c) have the required budgetary/financial resources to be able to carry out its responsibilities effectively; and

(d) be provided with sufficient and regular training in the area of compliance.

**Compliance Function Responsibilities**

**Principle 7**

**The responsibilities of the financial institution's compliance function should be to assist senior management in managing effectively the compliance risks faced by the financial institution. Its specific responsibilities are set out below. If some of these responsibilities are carried out by staff in different departments, the allocation of responsibilities to each department should be clear.**

2.6 The compliance function shall assist the senior management in:

(a) ensuring that the financial institution operates with integrity and in compliance with applicable laws, regulations and other compliance obligations in Mauritius and outside Mauritius as relevant including, but not limited to, money laundering/terrorism financing and proliferation financing risks as well as with the compliance policy and the related policies, processes and procedures;

(b) the promotion of a strong compliance culture and in the implementation of an effective governance and risk management framework for compliance risk across the financial institution; and

(c) ensuring that changes in applicable laws, regulations and other compliance obligations are promptly disseminated within the financial institution and monitor compliance thereof.

2.7 With respect to anti-money laundering and the financing of terrorism and proliferation, the Head of Compliance and staff of the compliance function shall also discharge, as applicable, all responsibilities and requirements (assigned to the compliance function) under the Financial Intelligence and Anti-Money Laundering Act, the Financial Intelligence and Anti-Money Laundering Regulations 2018, the Guideline on Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation, the Financial Crimes Commission Act 2023 and other related legislative and regulatory requirements.

*Advice*

2.8 The compliance function shall advise senior management on the applicable laws, regulations and other compliance obligations and update them on developments in the area.

*Guidance and education*

2.9 The compliance function should assist senior management in:

(a) educating staff on applicable laws, regulations and other compliance obligations, and acting as a contact point for their queries on these; and

(b) providing guidance to staff, in writing where necessary, on compliance with applicable laws, regulations and other compliance obligations, and as relevant, in the drafting of policies, procedures, processes, compliance manuals, internal codes of conduct and other internal guidelines.

*Identification, measurement and assessment of compliance risk*

2.10 The compliance function shall:

(a) conduct relevant risk assessments to identify, document and assess the compliance risks related to the financial institution's business activities, including those associated with the development of new products and business practices, new types of business or customer relationships and material changes in the nature of such relationships;

(b) ensure that risk assessments are updated regularly and promptly in case of material incidents and developments;

(c) ensure that controls to manage and mitigate compliance risk are appropriate and operating effectively;

(d) oversee the implementation of risk mitigation plans and other instructions of the Bank;

(e) implement relevant indicators to measure compliance risk and supplement the compliance risk assessment; and

(f) assess the appropriateness of measures being taken to address identified gaps.

*Compliance Programme*

2.11 The compliance function should establish a compliance programme that sets out its planned activities, such as the implementation and review of specific policies and procedures, compliance risk assessment, compliance monitoring and testing and educating staff on compliance issues.

2.12 The compliance programme should be risk-based and be reviewed and approved annually by the board or the designated sub-committee[7].

*Monitoring and testing*

2.13 The monitoring and testing programme should cover the adequacy and effectiveness of the compliance risk management and governance framework. The monitoring and testing programme should be reviewed and approved annually by the board or the designated sub-committee[7].

2.14 The scope and frequency of compliance monitoring and testing should be risk-based. Compliance with all relevant laws, regulations, guidelines, reporting requirements, other instructions and other compliance obligations as well as adherence with the compliance policy should normally be covered within a three year period. Exceptions, if any, should be reported to the Board with reasons justifying the exception, and indicating the period within which each of the exempted items will be subject to a compliance review. In any case, compliance reviews should cover all items at least once in forty-eight months.

2.15 The results of the testing should be shared with the relevant senior management for corrective actions. A copy thereof should be shared with the Chief Risk Officer so that the latter can address the compliance risks at an Enterprise-wide level.

2.16 The results of the testing, the risk mitigation plan and the progress on the remediation plan should be reported to the board at least on a quarterly basis.

2.17 The compliance function shall, except if stated otherwise, test compliance with all obligations established through new or amended laws, regulations, guidelines, reporting requirements and other methods within one year from their effective date. The compliance function may also rely on reviews conducted by internal audit to scope their reviews.

*Reporting to Board*

2.18 The Head of Compliance should submit regular reports (at least on a quarterly basis) to the board or the relevant subcommittee of the board. The reports shall include the following, as applicable:

(a) the financial institution's compliance with applicable laws, regulations and other compliance obligations based on the monitoring and testing exercise of the compliance function;

(b) the financial institution's management of compliance risks;

(c) results of the compliance risk assessment made during the reporting period;

(d) changes in the compliance risk profile including relevant risk indicators;

(e) identified breaches, incidents, deficiencies and the impact (financial and non-financial) and the corrective measures taken/ to be taken;

[7]As applicable under paragraph 1.6

(f) changes in relevant legal, regulatory and other compliance obligations including measures being taken for timely compliance; and

(g) observations regarding the compliance culture prevailing across the financial institution.

## Section III – Relationship with Internal Audit

### Principle 8: Relationship with Internal Audit

**The scope and breadth of the activities of the compliance function should be subject to periodic review by the internal audit function.**

3.1 The compliance function should be subject to an independent review by the internal audit function and hence these two should be separate.

3.2 The risk assessment methodology of the internal audit function should include compliance risk. The audit programme should cover adequacy and effectiveness of the compliance function and testing of controls commensurate with the perceived level of compliance risk.

3.3 The internal audit function should keep the Head of Compliance informed, for appropriate follow-up, of any audit findings and incidents relating to compliance that it observes or detects during the course of audits of other functions or departments in the financial institution.

## Section IV – Cross-border Operations

### Principle 9: Cross-border issues

**Financial institutions should comply with applicable laws and regulations in all jurisdictions in which they conduct business, and the organisation and structure of the compliance function and its responsibilities should be consistent with local legal and regulatory requirements.**

4.1 Compliance functions shall also assist the senior management in complying with the relevant local laws, regulations and other compliance obligations when the financial institution conducts business in foreign jurisdictions.

4.2 The Head of Compliance and/or relevant staff in the compliance function should have the requisite knowledge of the applicable laws, regulations and other compliance obligations in relevant foreign jurisdictions.

4.3 Financial institutions shall establish an appropriate compliance function in subsidiaries established outside Mauritius which report to the group Head of Compliance in Mauritius.

## Section V – Outsourcing

5.1. Financial institutions shall not outsource the activities of the compliance function. However, exceptions for certain types of intra-group outsourcing may be allowed. This would be considered on a case-by-case basis. Financial institutions that intend to outsource the aforesaid activities, within the group, are required to seek prior authorization of the Bank and to consider the requirements of the Guideline on Outsourcing by Financial Institutions.

5.2. The board of directors, senior management and Head of Compliance shall ensure compliance with all applicable legal, regulatory and other compliance obligations when a financial institution enters into outsourcing arrangements and/or has recourse to services provided by third parties.

## Section VI – Regulatory Reporting / Approvals

6.1. Financial institutions shall comply with the requirements of Section 46 of the Banking Act 2004 with respect to the appointment of the Head of Compliance.

6.2. Financial institutions should promptly, not later than one week, inform the Bank, in writing of :

(a) the resignation of the Head of Compliance and provide the reasons for the resignation;

(b) the dismissal/transfer of the Head of Compliance and provide the reasons; and

(c) any material compliance incidents and issues that may arise within their organisation.

## Section VII - Branches and Subsidiaries of Foreign Banks

7.1. Branches and subsidiaries of foreign banks:

(a) may adopt the compliance policies of their parent bank provided that they meet the requirements of this Guideline, are appropriate for their business strategies and adequately address their compliance risks;

(b) may rely on the resources of the parent bank as long as they are able to demonstrate appropriate independence and oversight on the compliance related tasks performed by the parent bank; and

(c) should ensure that any arrangements with the parent bank do not impede effective supervision by the Bank.

7.2. Regardless of the extent to which specific tasks of the compliance function are performed by the parent bank, the board and senior management remain responsible for compliance by the financial institution with all applicable laws, regulations, other compliance obligations and requirements of this Guideline.

## Section VIII – Transitional Arrangements

8.1. Financial Institution shall ensure compliance with the requirements of this Guideline by 31 May 2025.

**Bank of Mauritius**
**12 November 2024**