BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Compliance

Applicable to:
1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed international Islamic banks
5. Licensed insurers
6. Licensed takaful operators
7. Prescribed development financial institutions
8. Financial holding companies

Issued on: 2 October 2015 BNM/RH/PD 028-9

TABLE OF CONTENTS

PART A OVERVIEW 1
1 Introduction 1
2 Applicability 1
3 Legal provisions 2
4 Effective date 2
5 Interpretation 2

PART B POLICY REQUIREMENTS 4
6 Responsibilities of the board and senior management 4
7 Organisation of the compliance function 6
8 Responsibilities of the compliance function 8
9 Responsibilities of the internal audit function 10

PART A OVERVIEW

1 Introduction

1.1 A strong compliance culture reflects a corporate culture of high ethical standards and integrity in which the board and senior management lead by example. A financial institution should hold itself to high standards in carrying on business, and at all times observe both the spirit and the letter of the law and regulations. Failure to effectively manage compliance risk may result in adverse consequences for the financial institution's customers, shareholders, officers and the financial institution itself.

1.2 Compliance is the responsibility of all officers within a financial institution. All business lines and functions within a financial institution must carry out their responsibilities to ensure the effective management of compliance risk:

(a) business lines, through appropriate managerial and supervisory controls, are primarily responsible for managing compliance risk inherent in the day-to-day activities, processes and systems of the financial institution for which they are accountable;

(b) the compliance function is responsible for ensuring that controls to manage compliance risk are adequate and operating as intended. It is also responsible for assessing and monitoring of compliance risk faced by the financial institution; and

(c) the internal audit function is responsible for providing independent assurance to the board and senior management on the quality and effectiveness of the institution's overall internal controls, risk management and governance systems and processes, including those instituted by the compliance function.

1.3 The objective of the requirements in this policy document is to promote the safety and soundness of financial institutions by minimising financial, reputational and operational risks arising from legal and regulatory non-compliance.

1.4 This policy document sets out the following:

(a) expectations on the board and senior management to oversee and ensure the effective management of compliance risk, including the establishment of a compliance function and the position of chief compliance officer; and

(b) key features and responsibilities of the compliance function to support the effective management of compliance risk.

2 Applicability

2.1 This policy document is applicable to all financial institutions as defined in paragraph 5.2.

3 Legal provisions

3.1 This policy document is issued pursuant to–

(a) section 47(1), section 115 and section 266 of the Financial Services Act 2013 (FSA);

(b) section 57(1), section 127 and section 277 of the Islamic Financial Services Act 2013 (IFSA); and

(c) section 41 and section 126 of the Development Financial Institutions Act 2002 (DFIA).

4 Effective date

4.1 This policy document comes into effect on 1 January 2017.

5 Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, IFSA or DFIA, as the case may be, unless otherwise defined in this policy document.

5.2 For the purpose of this policy document–

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action;

"G" denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted;

"board" means the board of directors of a financial institution, including a committee of the board where the responsibilities of the board set out in this policy document have been delegated to such a committee;

"senior management" refers to the chief executive officer and senior officers of a financial institution;

"chief compliance officer" or **"CCO"** means the senior officer of a financial institution, however styled, who is the central point of authority for a financial institution's compliance matters and is responsible for providing an institution-wide view on the management of compliance risk;

"compliance function" refers to officers carrying out compliance function responsibilities of a financial institution, as described in paragraphs 8.4 to 8.11, including the CCO;

"compliance risk" means the risk of legal or regulatory sanctions, financial loss or reputational damage which a financial institution may suffer as a result of its failure to comply with legal and regulatory requirements applicable to its activities;

"control function" refers to a function that has a responsibility independent from business lines to provide objective assessment, reporting or assurance. This includes the risk management function, the compliance function and the internal audit function;

"financial institution" means–
(a) a licensed person under the FSA;
(b) a licensed person under the IFSA;
(c) a development financial institution prescribed under the DFIA; and
(d) a financial holding company;

"legal and regulatory requirements" means all laws, rules, standards and regulatory requirements (including any ruling of the Shariah Advisory Council) relevant to a financial institution's activities in all jurisdictions in which the financial institution, or any of its branches or subsidiaries, conducts activities.

PART B POLICY REQUIREMENTS

6 Responsibilities of the board and senior management

G 6.1 The board and senior management assume primary roles in fostering a strong compliance culture within a financial institution by ensuring that officers understand their responsibilities in respect of compliance and feel comfortable raising concerns without fear of retaliation. In this respect, the board and senior management should create an environment which not only ensures that the financial institution and its officers comply with legal and regulatory requirements, but also encourages the ethical conduct that underlies such requirements.

Responsibilities of the board

S 6.2 The board is responsible for overseeing the management of a financial institution's compliance risk. In order to fulfil this duty, the board must–

(a) approve the financial institution's compliance policy and oversee its implementation;

(b) approve the establishment of the compliance function and the position of the CCO, and ensure that the compliance function and the CCO are provided with appropriate standing, authority and independence;

(c) discuss compliance issues regularly, ensuring that adequate time and priority is provided in the board agenda to deliberate compliance issues and that such issues are resolved effectively and expeditiously; and

(d) at least annually, evaluate the effectiveness of the financial institution's overall management of compliance risk, having regard to the assessments of senior management and internal audit, as well as interactions with the CCO.

S 6.3 In relation to the position of the CCO, the board must–

(a) approve the appointment, remuneration and termination of the CCO[1];

(b) ensure that the CCO has sufficient stature to allow for effective engagement with the CEO and other members of senior management;

(c) engage with the CCO on a regular basis[2] to provide the opportunity for the CCO to discuss issues faced by the compliance function;

(d) provide the CCO with direct and unimpeded access to the board;

(e) ensure that the CCO is supported with sufficient resources, including competent officers, to perform his duties effectively; and

(f) where the CCO also carries out responsibilities in respect of other control functions[3], be satisfied that a sound overall control environment will not be compromised by the combination of responsibilities performed by the CCO.

---

1 Refer to the policy documents on *Fit and Proper Criteria* issued on 28 June 2013 and *Guidelines on Fit and Proper for Key Responsible Persons for Development Financial Institutions* issued on 15 September 2011.

2 The board should also consider engaging the CCO without the presence of other members of senior management from time to time.

3 Refer to paragraphs 7.3 and 7.4.

Responsibilities of senior management

S 6.4 Senior management is collectively responsible for the effective management of a financial institution's compliance risk. In discharging this responsibility, senior management must–

(a) establish a written compliance policy and ensure that it is kept up to date;

(b) communicate the policy to all officers and ensure that appropriate remedial or disciplinary actions are taken if the compliance policy is breached;

(c) establish a compliance function commensurate with the size, nature of operations and complexity of the financial institution, having regard to the requirements in paragraphs 7 and 8;

(d) provide sufficient resources for the compliance function, including officers with the appropriate competencies and experience;

(e) ensure that the compliance function is able to secure assistance from other functions with specific expertise (for example, legal, Shariah review or risk management) and has clear authority to engage with any officers and obtain access to relevant information for purposes of discharging its responsibilities;

(f) ensure that the compliance function is able to engage relevant external expertise to undertake compliance assessments in specific areas[4] where necessary;

(g) ensure that the compliance function is kept informed of any organisational developments to facilitate the timely identification of compliance risk;

(h) report to the board regularly on compliance issues and promptly on any material incidents of non-compliance (for example, failures that may attract a significant risk of legal or regulatory sanction);

(i) report to the board at least annually on the effectiveness of the financial institution's overall management of compliance risk in such a manner as to assist the board in carrying out its responsibilities as set out in paragraph 6.2(d); and

(j) inform the board of the CCO's cessation from office and the reasons leading to the cessation.

S 6.5 In relation to paragraph 6.4(a), senior management must set out principles to be followed by all officers and explain the main processes by which compliance risk is identified and managed. In particular, senior management must make clear in the compliance policy that the primary responsibility to manage compliance risk lies with the business lines and that the establishment of the compliance function does not substitute the primary role of business lines in managing compliance risk. This includes the responsibility of business lines to own, develop and update systems, policies, processes and procedures to manage compliance risk inherent in business activities.

[4] For example, to conduct investigations of possible incidents of non-compliance.

S 6.6 For the purpose of paragraph 6.4(h), senior management must include the following information in its reports:

(a) an identification and assessment of the compliance issues faced by the financial institution. These issues include any significant shortfalls arising from the implementation or execution of internal controls put in place to manage compliance risk;

(b) compliance issues involving any member of senior management of the financial institution, and the status of any associated investigations or other actions being taken; and

(c) plans to manage compliance issues, as well as the need for any additional policies or procedures to deal with any new compliance risk.

S 6.7 In relation to paragraph 6.4(i), senior management must take into account the outcome of the compliance function's assessment of compliance risk as described in paragraph 8.8. The reports must, at minimum, include an assessment of the key compliance risks faced by the financial institution and their implications on the financial institution's capacity to manage compliance risk going forward.

7 Organisation of the compliance function

S 7.1 A financial institution must organise its compliance function in a manner that allows compliance risk to be managed effectively, taking into account the size, nature of operations and complexity of the financial institution's business and the legal and regulatory environment in the jurisdictions or sectors in which it has operations.

S 7.2 Where compliance function responsibilities are shared between a dedicated compliance unit and other control functions–

(a) the allocation of the compliance function responsibilities, including that for timely communication and escalation of compliance issues to senior management and the board, must be clearly defined and documented in the compliance policy;

(b) the CCO must have overall responsibility for coordinating the identification and management of compliance risk at the institution-wide level, and ensuring that compliance monitoring and testing are carried out consistently across the institution;

(c) for the purpose of paragraph 7.2(b), the CCO must have a sound understanding of compliance risks which are under the purview of other control functions, including an understanding of controls applied to manage these risks;

(d) arrangements for coordination among the control functions with the CCO and the compliance unit must be in place to ensure that the CCO is able to perform his responsibilities effectively. Arrangements should promote a view and approach to the management of compliance risk that is consistent across the organisation, including through adequate information flows and avenues to seek advice on compliance issues; and

(e) senior management must ensure that officers in other control functions have the capacity and expertise to deliver their broader mandates while providing adequate focus to their compliance function responsibilities.

S 7.3 Where the CCO also assumes responsibilities for other control functions, the CCO must ensure that his independence and ability to provide sufficient time, focus and commitment to his responsibilities in respect of the compliance function is not impaired.

S 7.4 In relation to paragraphs 7.2 and 7.3–

(a) the board must approve the sharing of compliance function responsibilities between a dedicated compliance unit and other control functions; and

(b) compliance function responsibilities cannot be shared with, nor can the CCO assume responsibilities for, internal audit as such practices would render the independent review process described in paragraph 9.1 ineffective.

S 7.5 A large financial institution is required to establish a unit or department, headed by the CCO, which is dedicated to carrying out the compliance function responsibilities set out in paragraph 8. This is to provide necessary focus on the management of compliance risk in view of the inherent complexity and scale of operations of large financial institutions.

S 7.6 Notwithstanding paragraph 7.3, the CCO of a large financial institution is not allowed to assume the responsibilities of other control functions.

Independence

S 7.7 The compliance function must be independent of business lines in order to carry out its role as a control function effectively. As such, a financial institution must ensure that the compliance function is not placed in a position where there are real or potential conflicts in respect of its scope of responsibilities, reporting lines or remuneration.

S 7.8 A financial institution must ensure that the remuneration of the CCO and officers performing compliance functions are structured in a way that does not compromise their independence (for example, the remuneration must not be related to the financial performance of any particular business line) and must be primarily based on the achievement of their compliance function responsibilities.

G 7.9 A constructive and cooperative working relationship between the compliance function and business lines can improve the overall identification and management of compliance risk. In practice, this can involve the direct participation of the compliance function in providing legal and regulatory input to business processes or decisions[5].

[5] For example, through representation on a new products committee.

S 7.10 Where such arrangements referred to in paragraph 7.9 exist, a financial institution must ensure that–

(a) the compliance function is not placed in a position of conflict;

(b) the accountability of the compliance function is properly documented[6]; and

(c) the compliance function is not prevented from highlighting compliance issues relating to any business decisions to the board or senior management, where necessary.

Resources

S 7.11 Officers undertaking compliance function responsibilities must have the necessary qualifications and experience. In particular, they must have a sound understanding of relevant legal and regulatory requirements and the implications of such requirements on a financial institution's operations. This includes possessing relevant local knowledge and expertise in respect of the legal and regulatory requirements applicable in the jurisdictions in which the financial institution conducts its activities.

S 7.12 A financial institution must ensure that the compliance function is kept abreast of developments in legal and regulatory requirements by undertaking regular and systematic programmes and training.

G 7.13 As one of the means to develop a strong compliance function, a financial institution should consider mandating or encouraging compliance function officers to possess accredited qualifications in the area of compliance.

8 Responsibilities of the compliance function

S 8.1 A financial institution must ensure that the scope of responsibilities of the compliance function sufficiently cover all businesses, branches and subsidiaries, whether in or outside Malaysia and whether or not an activity is carried out by the financial institution itself or by a third party on its behalf. This means that a financial institution which conducts business internationally through local subsidiaries or branches, or in other jurisdictions where it does not have a physical presence, must also ensure compliance with all local legal and regulatory requirements applicable in those jurisdictions.

S 8.2 Where a financial institution has operations in more than one jurisdiction, it must consider the need to establish a local compliance unit or department to discharge independent compliance function responsibilities in respect of its operations in each of these jurisdictions. Where a local compliance unit or department is established, there must be appropriate mechanisms for coordination between the local compliance unit or department and the compliance function of the financial institution, to ensure that compliance risk is managed effectively.

---

[6] In the case of a committee, the role of the compliance function may be outlined in the terms of reference or charter.

S 8.3 The manner in which the compliance function discharges its responsibilities must be reflective of its assessment of the level and impact of the compliance risk facing a financial institution. Accordingly, the compliance function must give greater focus to areas where compliance risk is assessed to be high, while preserving appropriate coverage of all compliance risks identified.

Identification, assessment and monitoring of compliance risk

S 8.4 The compliance function must identify and assess the compliance risk associated with a financial institution's activities. This requires the compliance function to have adequate knowledge and exposure to key business processes of the financial institution[7] and keep up with material changes in the financial institution's business.

S 8.5 The compliance function must use a range of indicators to identify, assess and systematically monitor the level of compliance risk. These indicators may be qualitative or quantitative in nature and may include, but are not limited to, trends in customer complaints, irregular trading or payments activity and assessments by regulatory authorities.

S 8.6 The compliance function must perform appropriate tests to evaluate the adequacy of internal controls put in place to manage compliance risk[8] and promptly follow up on any identified deficiencies and plans to address such deficiencies.

S 8.7 Where the testing of internal controls is performed by the compliance function on a sampling basis–

(a) such testing must be commensurate with the level of compliance risk identified in the business process (for example, as reflected in the frequency or volume of transactions); and

(b) the sample must be representative of the different types of internal controls implemented at different stages of business processes within a financial institution.

Reporting of compliance risk

S 8.8 The CCO must report to senior management on a regular basis the findings and analyses of compliance risk. The report must include at minimum–

(a) the results of the compliance risk assessment undertaken during the assessment period, highlighting key changes in the compliance risk profile of a financial institution as well as areas where greater attention by senior management would be needed;

(b) a summary of incidents of non-compliance and deficiencies in the management of compliance risk in various parts of the financial institution;

(c) an assessment of the impact (both financial and non-financial) of such incidents on the financial institution (for example, fines, administrative or

---

[7] For example, the development of new products, the strategic planning process (including mergers and acquisitions and entry into new lines of business), or the establishment of customer relationships and any material changes in the nature of such relationships.

[8] This may include validating risk control self-assessment reports submitted to the compliance function.

otherwise, or other disciplinary actions taken by any regulatory authority in respect of any officers of the financial institution);

(d) recommendations of corrective measures to address incidents of non-compliance and deficiencies in the management of compliance risk, including disciplinary actions;

(e) a record of corrective measures already taken and an assessment of the adequacy and effectiveness of such measures; and

(f) insights and observations regarding the compliance culture that exists in the organisation or in specific parts of the organisation that may give rise to compliance concerns.

S 8.9 The CCO must ensure that the reports referred to in paragraph 8.8 are readily available to the internal audit function of the financial institution, the Bank and other regulatory authorities upon request.

Advisory

S 8.10 The compliance function must advise the board, senior management and officers on legal and regulatory requirements. This includes keeping them informed on the developments affecting legal and regulatory requirements and providing the board and senior management with an assessment of their implications on a financial institution's compliance risk profile and capacity to manage compliance risk going forward.

Guidance and training

S 8.11 The compliance function is responsible for ensuring that adequate training is provided to officers of a financial institution on relevant legal and regulatory requirements governing the financial institution's activities. Such training must be timely and must clearly explain how the requirements apply in the specific context of the financial institution's operations. The compliance function must be able to provide guidance to officers of the financial institution on the implementation of internal controls to manage compliance risk.

9 Responsibilities of the internal audit function

S 9.1 A financial institution must ensure that there is a clear separation of the internal audit function and other functions carrying out compliance function responsibilities. Compliance risk must be included in the risk assessment methodology of the internal audit function, and an audit programme that covers the adequacy and effectiveness of the other functions carrying out compliance function responsibilities should be established, including testing of controls commensurate with the perceived level of risk.

S 9.2 The internal audit function is required to inform senior management, including the CCO, of any incidents of non-compliance which it discovers.