BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

# **Compliance**
# Concept Paper

Issued on: 25 September 2014

## TABLE OF CONTENTS

The absence of an effective compliance risk management framework exposes a financial institution's customers, shareholders, employees and the financial institution itself to serious risks. An evolving regulatory landscape and the expansion of operations into new markets have increased financial institutions' vulnerability to compliance risk and underscore the need for financial institutions' capacity to manage compliance risk to be continuously strengthened.

Failure to manage compliance risk effectively may result in sanctions by regulators and litigation by third parties, resulting in the diversion of focus and management time and resources to unproductive problem resolution.

The Bank is issuing this concept paper on compliance to promote higher standards of compliance in all financial institutions which are licensed persons under the Financial Services Act 2013 and Islamic Financial Services Act 2013, and development financial institutions prescribed under the Development Financial Institutions Act 2002. The requirements in this concept paper complement the Bank's risk-based supervisory framework, and seek to, among others, ensure that effective compliance policies and procedures are followed and that senior management of the financial institutions above take appropriate corrective action when compliance failures are identified.

The proposed requirements emphasise strong ownership of compliance risk by business lines, the establishment of a compliance function which is supported by sufficient resources and more effective interaction between the compliance function and business lines.

The proposals in this concept paper are consistent with the requirements under the Core Principles for Effective Banking Supervision and Insurance Core Principles respectively issued by the Basel Committee on Banking Supervision and the International Association of Insurance Supervisors.

Issued on: 25 September 2014

The Bank invites written comments on this concept paper, including suggestions for particular issues/areas to be clarified or elaborated further and any alternative proposals that the Bank should consider. To facilitate the Bank's assessment, please support each comment with a clear rationale, accompanying evidence or illustration, as appropriate.

In addition to providing general feedback, financial institutions are requested to respond to the specific questions set out in this concept paper.

In finalising the requirements in this concept paper, the Bank will also subsequently update other related policy documents (for example, Principle 8 of Risk Governance and paragraph 6.2 of the Guidelines on Internal Audit Function of Licensed Institutions).

Responses must be submitted by 25 November 2014 to:

Pengarah
Jabatan Dasar Kewangan Pruden
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Email: pfpconsult@bnm.gov.my

Electronic submission is encouraged. Submissions received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

# 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's compliance function forms an integral part of its control functions, complementing other functions such as risk management. 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 a financial institution's customers, shareholders, employees and the financial institution itself.

**Policy objective**

1.2 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.

**Scope of policy**

1.3 This policy document sets out:

(i) expectations on the board and senior management to oversee and ensure the effective management of compliance risk;

(ii) key features of the compliance function to support the effective management of compliance risk; and

(iii) the responsibilities of the compliance function.

## 2 Applicability

2.1 This policy document is applicable to:

(i) a licensed person under the Financial Services Act 2013 (FSA);

(ii) a licensed person under the Islamic Financial Services Act 2013 (IFSA); and

(iii) a development financial institution prescribed under the Development Financial Institutions Act 2002 (DFIA).

These institutions are collectively referred to as “financial institutions” in this policy document.

## 3 Legal provisions

3.1 The requirements in this policy document are specified pursuant to:

(i) section 47(1) of FSA;

(ii) section 57(1) of IFSA; and

(iii) section 41 of DFIA.

## 4 Effective date

4.1 The policy document will be effective upon issuance of the final document.

## 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 document.

5.2 For the purposes of this policy document-

**“S”** denotes a standard, requirement or specification that must be complied with. Failure to comply may result in one or more enforcement actions;

**“G”** denotes guidance which may consist of such information, advice or recommendation intended to promote common understanding and sound industry practices which are encouraged to be adopted;

**“board”** means the board of directors of a financial institution, or a committee of the board where the responsibilities of the board set out in the policy document have been delegated to such committee;

**“senior management”** refers to the chief executive officer and senior officers of a financial institution;

**“chief compliance officer”** means the senior officer of a financial institution, however styled, who is primarily responsible for the compliance function of the financial institution;

**“compliance function”** refers to the chief compliance officer and staff or groups of staff carrying out compliance function responsibilities of a financial institution, as described in paragraphs 8.3 to 8.14;

**“compliance policy”** refers to a written document (or a set of written documents) which sets out principles to be followed by all staff, explains the main processes by which compliance risk is managed and sets out the roles of business lines, the chief compliance officer and the compliance function in managing compliance risk within a financial institution;

**“compliance risk”** means the legal and regulatory risk arising from non-compliance to legal and regulatory requirements; and

**“legal and regulatory requirements”** means all laws, rules, standards and other regulatory requirements (including Shariah) 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

6.1 The board and senior management assume primary roles in fostering a strong compliance culture within the financial institution. Both the board and senior management should set the "tone at the top" by emphasising the values of honesty and integrity in the dealings and activities of the financial institution, and the behaviour of its staff. In addition to leading by example, the board and senior management must ensure that employees 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 employees comply with legal and regulatory requirements, but also encourages the ethical conduct that underlies such requirements.

**Responsibilities of the board**

**S** 6.2 It is the responsibility of the board to oversee the management of the financial institution's compliance risk. In order to fulfil this duty, the board must-

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

(ii) approve the establishment of a compliance function in the financial institution and ensure that it is provided with appropriate standing, authority and independence;

(iii) establish the position of the chief compliance officer (CCO);

(iv) discuss compliance risk issues regularly, ensure that sufficient time is allocated in the board meeting agenda for deliberation of such issues and ensure that such issues are resolved effectively and expeditiously; and

(v) evaluate the effectiveness of the financial institution's overall management of compliance risk at least annually.

**S** 6.3 In relation to paragraph 6.2(iii), the board must-

(i) oversee the appointment, remuneration and termination of the CCO, and be actively involved in his performance reviews[1];

(ii) ensure that the appointed CCO is of sufficient stature and seniority to allow for regular and timely communication with the CEO and other members of senior management;

(iii) engage with the CCO on a regular basis, without the presence of other members of senior management, to provide the opportunity for the CCO to discuss issues faced by the compliance function;

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

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

(vi) where the CCO also carries out responsibilities in respect of other control functions, be satisfied that a sound overall control environment will not be compromised by the combination of responsibilities for control functions being carried out by a single individual.

**Responsibilities of senior management**

**S** 6.4 Senior management must be responsible for the effective management of the financial institution's compliance risk. In carrying out this responsibility, senior management must-

(i) establish a compliance policy, communicate the policy to all staff and ensure that appropriate remedial or disciplinary actions are taken if the compliance policy is breached;

(ii) establish a compliance function commensurate with the size, nature of operations and complexity of the financial institution;

(iii) provide sufficient resources, including competent staff for the compliance function and ensure that the compliance function is able to secure assistance from other functions with specific expertise (for example, legal or internal audit);

(iv) report to the board regularly on compliance risk issues and promptly on

[1] This is to be read together with the policy documents on *Fit and Proper Criteria* and *Guidelines on Fit and Proper for Key Responsible Persons for Development Financial Institutions*.

any material incidences of non-compliance (for example, failures that may attract a significant risk of legal or regulatory sanction);

(v) 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(v); and

(vi) 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(i), the compliance policy must make clear that it is the primary responsibility of risk-taking functions and business lines to ensure legal and regulatory compliance. This includes the responsibility of risk-taking functions and business lines to own, develop and update systems, policies, processes and procedures which act as internal controls to manage compliance risk. In particular, senior management must ensure that the compliance function established under the requirements of paragraph 7 reinforces and complements, and does not substitute, the primary role of risk-taking functions and business lines to ensure legal and regulatory compliance. Senior management must also ensure that the compliance function is kept informed of any organisational developments to facilitate the early identification of compliance risks as required under paragraph 8.3.

**S** 6.6 In relation to paragraph 6.4(iv), reports by senior management to the board must include an identification and assessment of the compliance risk issues faced by the financial institution and plans to manage them. Compliance risk issues include any shortfalls relating to the internal controls put in place to manage compliance risk or the implementation or execution of such internal controls, whether or not these shortfalls have resulted in incidences of non-compliance. Plans to manage compliance risk issues must address these shortfalls, as well as the need for any additional policies or procedures to deal with any new compliance risks.

**G** 6.7 In relation to paragraph 6.4(v), reports by senior management to the board should consider the outcomes of the compliance function's assessment of compliance risk as described in paragraph 8.9 and, in addition, should include:

(i) an assessment of the key compliance risks faced by the financial institution (for example, arising from legal and regulatory developments) and their implications on the financial institution's capacity to manage compliance risk going forward; and

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

6.8 For purposes of the requirement in paragraph 6.4(vi) above and in accordance with section 62 of the FSA and section 71 of the IFSA, a licensed person must notify the Bank in writing upon the cessation of its CCO and the reasons for it not later than seven days from the date of the financial institution giving or receiving the notice of the cessation.

**S** 6.9 For purposes of the requirement in paragraph 6.4(vi) above, a development financial institution prescribed under the DFIA must notify the Bank in writing upon the cessation of its CCO and the reasons for it not later than seven days from the date of the development financial institution giving or receiving the notice of the cessation.

## 7 Compliance function

7.1 An effective compliance function is one that is independent and is equipped with sufficient resources.

**S** 7.2 The compliance function must be organised in a manner which:

(i) 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; and

(ii) ensures that the compliance function is supported with sufficient resources, including competent staff.

***Independence***

**S** 7.3 The compliance function must be independent of risk-taking functions and business lines in order to carry out its role as a control function effectively. As such, the compliance function must not be placed in a position where there are real or potential conflicts in respect of its scope of responsibilities, reporting lines or remuneration.

**S** 7.4 The remuneration of the CCO and staff of the compliance function must be structured in a way that is primarily based on the performance of the compliance function in carrying out its responsibilities, consistent with paragraphs 65 and 66 of the policy document on Risk Governance.

7.5 Independence should not preclude the compliance function from working closely with senior management and staff in the various business lines. A cooperative working relationship between the compliance function and business lines can help to identify and manage compliance risk at an early stage. The requirements in paragraphs 7.6 to 7.11 seek to enable these cooperative relationships to be leveraged on in a way which would not undermine the independence of the compliance function.

**S** 7.6 If the compliance function is combined with, or consists of staff who also carry out responsibilities in respect of other functions or departments (for example, legal or risk management), then-

(i) the allocation of compliance function responsibilities to each function or department, and staff involved, must be clear and documented;

(ii) there must be appropriate mechanisms for coordination among the functions or departments and with the CCO, to ensure that the CCO is able to perform his responsibilities effectively; and

(iii) staff must not be placed in a position where there are real or potential conflicts of interest between their compliance function responsibilities and other responsibilities.

**S** 7.7 Where compliance function responsibilities are performed by staff residing in risk-taking functions or business lines, the conditions in paragraph 7.6 must be met and such staff must have a reporting line to the CCO with respect to their compliance function responsibilities.

**S** 7.8 The CCO, as head of the compliance function, is not precluded from assuming responsibilities for other control functions (other than the internal audit function[2]), subject to him maintaining his independence and being able to provide sufficient time and commitment to, and focus on, his responsibilities in respect of the compliance function.

**G** 7.9 A financial institution may consider it optimal to organise its compliance function within its risk management function, given the close relationship between compliance risk and certain aspects of operational risk. Alternatively, a financial institution may consider it optimal to maintain separate compliance and risk management functions, with appropriate mechanisms for cooperation between the two functions on compliance matters.

**S** 7.10 Regardless of how a financial institution organises its compliance function, the structures of and reporting lines within and among the compliance, risk management and internal audit functions must be designed in a manner that supports the timely communication of issues which have an impact on the effectiveness of the financial institution's risk management framework and internal control environment, and ensures the prompt escalation of such issues to the board and senior management.

[2] The CCO must not be primarily responsible for internal audit as this would render the independent review process (as described in paragraphs 9.1 and 9.2) ineffective.

**S** 7.11 For a large financial institution, a dedicated unit or department which is primarily responsible for carrying out compliance function responsibilities must be set up, with a CCO whose sole responsibility is in respect of the compliance function, to provide the necessary focus on compliance risk.

The definition of a large financial institution for the purposes of this policy document will be consistent with that used for the purposes of the policy document on *Operational Risk Management*. The Bank is currently reviewing feedback on the concept paper on *Operational Risk Management* and will take into account the comments provided in refining the definition.

It is crucial for the compliance function to remain independent in carrying out its responsibilities. While this policy document does not intend to prescribe a particular structure for the compliance function, the Bank notes that some financial institutions may choose to organise their compliance functions in a manner which involves staff in other functions or departments. The questions below are intended to assess the need for further guidance in this area.

**Question 1**

Please describe the manner in which your institution's compliance function is organised (for example, a standalone department, combined with another department or function, group-wide arrangements) and whether any compliance function responsibilities (paragraphs 8.3 to 8.14) are carried out by staff residing in risk-taking functions or business lines.

**Question 2**

Where compliance function responsibilities are carried out by staff residing in risk-taking functions or business lines, please describe the current roles of these staff and measures put in place to preserve the independence of the compliance function (for example, in respect of allocation of responsibilities, remuneration structure, reporting line). Please also elaborate on changes that have to be made in respect of such roles or measures to meet the above requirements.

**G** 7.12 A financial institution with operations in more than one jurisdiction should consider the need to establish a local compliance unit or department to discharge compliance function responsibilities in respect of its operations in each of these jurisdictions. There should 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.

**S** 7.13 The compliance function must be given the explicit right to engage with any staff and obtain access to relevant records or files for purposes of discharging its functions.

The cross-border expansion of financial institutions has increased the exposure of financial institutions to compliance risk (for example, arising from legal and regulatory requirements which the financial institution must adhere to across different jurisdictions). The question below is intended to allow the Bank to gauge any challenges which may be faced by a financial institution and to assess the need for further guidance in this area.

**Question 3**

Please describe any challenges which may be faced in coordinating the management of compliance risk (for example, in the regular reporting of compliance risk issues) for branches or subsidiaries located outside of Malaysia.

***Resources***

**S** 7.14 The staff in the compliance function must have the necessary qualifications and experience. In particular, the staff in the compliance function must have a sound understanding of relevant legal and regulatory requirements and the implications of such requirements on the 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 activities.

**S** 7.15 There must be regular and systematic programmes and training to keep the compliance function abreast with developments in such legal and regulatory requirements.

**G** 7.16 As a means to developing a strong compliance function, financial institutions should consider mandating or encouraging staff to possess internationally-accredited qualifications in the area of compliance.

**S** 7.17 In certain circumstances, it may be necessary to engage external expertise to undertake compliance assessments in specific areas (for example, to conduct investigations of possible incidences of non-compliance). The compliance function must be allowed to engage such external expertise without undue impediment, subject to the appropriate board, senior management or regulatory approvals.

## 8 Responsibilities of the compliance function

**S** 8.1 The responsibilities of the compliance function must be discharged in a manner that sufficiently covers all businesses, branches and subsidiaries, whether in Malaysia or otherwise, as well as all outsourced activities of the financial institution.

**S** 8.2 This shall mean 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 to all local legal and regulatory requirements applicable in those jurisdictions.

***Identification, assessment and monitoring of compliance risk***

**S** 8.3 The compliance function must identify and assess the compliance risks associated with the financial institution's business activities. This requires the compliance function to have adequate knowledge and exposure to key business processes of the financial institution (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 or material changes in the nature of such relationships) and keeping up with material changes in the financial institution's business, where appropriate.

The involvement of the compliance function in the early identification of compliance risk is essential. However, it must be clear that participation of the compliance function in any business decision making is intended to provide input on the implications of the decision from a legal and regulatory compliance perspective. It does not absolve business lines of their compliance responsibilities in such decisions. The question below is intended to enable the Bank to understand current industry practice and to assess the need to provide further guidance in this area.

**Question 4**

To what extent is the compliance function currently involved in business decisions (for example, in committees which are involved in the development/approval of new products)? Please describe the role of the compliance function (for example, whether the compliance function has any role in endorsing decisions and how this role is differentiated from the responsibilities assumed by risk-taking functions for business decisions). Are there any specific measures that your institution takes to ensure that both the risk-taking and compliance functions remain effective in managing compliance risk as envisaged in paragraph 6.5?

**S** 8.4 The compliance function should consider using a range of qualitative and quantitative indicators to systematically monitor and measure compliance risk and use such measurements to enhance the assessment of compliance risk, while also prompting senior management to develop a response to mitigate this risk.

**G** 8.5 In relation to paragraph 8.4, such indicators may include, but are not limited to, trends in customer complaints, irregular trading or payment activity and communication from regulatory authorities.

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

**S** 8.7 The compliance function must regularly perform sufficient testing on all internal controls put in place to manage compliance risk within the financial institution, to ensure that such controls are operating effectively.

**G** 8.8 Where the testing of internal controls is performed on a sampling basis:

(i) such testing should 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

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

***Reporting of compliance risk***

**S** 8.9 The outcomes of the compliance function's assessment of compliance risk, as described in paragraphs 8.3 to 8.8, must be reported to senior management on a regular basis and must be presented in a manner which is appropriate to the risk profile and activities of the financial institution. This report shall include at least:

(i) the results of the compliance risk assessment undertaken during the assessment period, including any changes in the compliance risk profile of the financial institution;

(ii) a summary of incidences of non-compliance and deficiencies in the management of compliance risk in various parts of the financial institution (for example, in risk-taking functions and business lines);

(iii) an assessment of the impact (both financial and non-financial) of such incidences on the financial institution (for example, fines or other disciplinary actions taken by any regulatory authority in respect of any staff of the financial institution);

(iv) a recommendation of corrective measures to address incidences of non-compliance and deficiencies in the management of compliance risk, including disciplinary actions;

(v) a record of corrective measures already taken and an assessment of the appropriateness of such measures; and

(vi) 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** 8.10 These outcomes must be properly documented and be made readily available to the internal audit function of the financial institution, the Bank and other regulatory authorities upon request.

***Advisory***

**S** 8.11 The compliance function must advise the board, senior management and staff on legal and regulatory requirements. This includes keeping them informed on legal and regulatory developments and providing the board and senior management with an assessment of their implications on the financial institution's compliance risk exposures and capacity to manage compliance risk going forward.

***Guidance, education and training***

**S** 8.12 The compliance function is responsible for ensuring that adequate training is provided to staff of the financial institution on relevant legal and regulatory requirements governing the financial institution's business 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 also provide guidance on the implementation of internal controls to manage compliance risk.

**G** 8.13 In this capacity, the compliance function acts as a contact point within the financial institution for addressing queries relating to such requirements.

**G** 8.14 For the avoidance of doubt, the relevant legal and regulatory requirements referred to in paragraph 8.12 should extend beyond the prevention of money laundering and terrorist financing.

## 9 Responsibilities of the internal audit function

**S** 9.1 The internal audit function of a financial institution must periodically review the adequacy and effectiveness of the compliance function[3] and the internal controls put in place to manage compliance risk. The internal audit function must report regularly to the board on the outcome of this periodic review.

**S** 9.2 The internal audit function must inform the CCO of any incidences of non-compliance which it discovers.

In line with the Bank's *Approach to Regulating and Supervising Financial Groups*, the Bank intends to implement group-level standards relating to risk management and internal controls.

**Question 5**

Please highlight any specific challenges and suggestions to address these challenges if the requirements in this concept paper were to be applied to a financial holding company.

[3] This entails the separation of the compliance function and the internal audit function.

<u>For financial institutions offering Islamic financial services</u>

**Question 6**

The Bank's *Shariah Governance Framework* specifies that the Shariah review function has the responsibility to assess whether activites and operations are carried out in accordance with Shariah. How is the Shariah review function currently organised, and what changes to the role of compliance function in respect of Shariah do you envisage given the proposals in this concept paper? Is there a need for the Bank to provide further guidance in this area?

**Question 7**

End-to-end Shariah compliance entails adherence to the underlying principles of Shariah, and not merely the legal and regulatory requirements. Given the responsibilities defined in the concept paper, what role should the CCO play in respect of compliance with Shariah?