



GUIDELINES FOR COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS

Date: 2 January 2018

CONTENTS

PRINCIPLES	3
I. BOARD OF DIRECTORS RESPONSIBILITIES FOR COMPLIANCE	4
II. SENIOR MANAGEMENT RESPONSIBILITIES FOR COMPLIANCE	5
III. COMPLIANCE FUNCTION PRINCIPLES	7
A. INDEPENDENCE	7
<i>Status</i>	7
<i>Head of Compliance</i>	8
<i>Conflicts of interest</i>	9
<i>Access to information and personnel</i>	9
B. RESOURCES	11
C. COMPLIANCE FUNCTION RESPONSIBILITIES	12
<i>Advice, guidance and education</i>	12
<i>Identification, measurement and assessment of compliance risk</i>	13
<i>Monitoring, testing and reporting</i>	13
<i>Statutory responsibilities and liaison</i>	13
<i>Compliance programme</i>	14
D. RELATIONSHIP WITH INTERNAL AUDIT	15
IV. OTHER MATTERS	16
A. CROSS-BORDER ISSUES	16
B. OUTSOURCING	17

PRINCIPLES

- Principle 1 : The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board must approve the bank's compliance policy, including a formal document establishing a permanent and effective compliance function. At least once a year, the board or a committee of the board must assess the extent to which the bank is managing its compliance risk effectively.
- Principle 2 : The bank's senior management is responsible for the effective management of the bank's compliance risk. The bank's senior management is responsible for establishing and communicating a compliance policy, for ensuring that it is observed, and for reporting to the board of directors on the management of the bank's compliance risk. To the above ends, the bank's senior management is responsible for establishing a permanent and effective compliance function within the bank as part of the bank's compliance policy.
- Principle 3 : The bank's compliance function must be independent.
- Principle 4 : The bank's compliance function must have the resources to carry out its responsibilities effectively.
- Principle 5 : The responsibilities of the bank's compliance function must be to assist senior management in managing effectively the compliance risks faced by the bank. If some of these responsibilities are carried out by staff in different departments, the allocation of responsibilities to each department must be clear.
- Principle 6 : The scope and breadth of the activities of the compliance function must be subject to periodic review by the internal audit function.
- Principle 7 : Banks must comply with applicable laws and regulations in all jurisdictions in which they conduct business, and the structure of the compliance function must be consistent with local legal and regulatory requirements.
- Principle 8 : Compliance must be regarded as a core risk management activity within the bank. Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the head of compliance.

I. BOARD OF DIRECTORS RESPONSIBILITIES FOR COMPLIANCE

Principle

1. The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board must approve the bank's compliance policy, including a formal document establishing a permanent and effective compliance function. At least once a year, the board or a committee of the board must assess the extent to which the bank is managing its compliance risk effectively.

Guidelines

- 1.1 A bank's compliance policy will not be effective unless the board promotes the values of honesty and integrity throughout the organisation. Compliance with applicable laws, rules and standards must be viewed as an essential means to this end. The board is responsible for ensuring that an appropriate policy is in place to manage the bank's compliance risk. The audit committee must oversee the implementation of the policy, including ensuring that compliance issues are resolved effectively and expeditiously by senior management with the assistance of the compliance function.
- 1.2 A branch of a foreign bank licensed as a bank in Brunei Darussalam (Brunei branch of a foreign bank) must provide the AMBD with a satisfactory explanation how the bank's board of directors and senior management formalize and discharge their respective oversight responsibilities in relation to the Brunei branch of the foreign bank. This includes their responsibilities in terms of these Guidelines.

II. SENIOR MANAGEMENT RESPONSIBILITIES FOR COMPLIANCE

Principle

2. The bank's senior management is responsible for the effective management of the bank's compliance risk. The bank's senior management is responsible for establishing and communicating a compliance policy, for ensuring that it is observed, and for reporting to the board of directors on the management of the bank's compliance risk. To the above ends, the bank's senior management is responsible for establishing a permanent and effective compliance function within the bank as part of the bank's compliance policy.

Guidelines:

- 2.1 The bank's senior management is responsible for establishing a written compliance policy that contains the basic principles to be followed by management and staff, and explains the main processes by which compliance risks are to be identified and managed through all levels of the bank. Clarity and transparency may be promoted by making a distinction between general standards for all staff members and rules that only apply to specific groups of staff.
- 2.2 The duty of senior management to ensure that the compliance policy is observed entails responsibility for ensuring that appropriate remedial or disciplinary action is taken if breaches are identified.
- 2.3 Senior management must, with the assistance of the compliance function:
 - (a) at least once a year, identify and assess the main compliance risk issues facing the bank and the plans to manage them. Such plans must address any shortfalls (policy, procedures, implementation or execution) related to how effectively existing compliance risks have been managed, as well as the need for any additional policies or procedures to deal with new compliance risks identified as a result of the annual compliance risk assessment;
 - (b) at least once a year, report to the board of directors or a committee of the board on the bank's management of its compliance risk, in such a manner as to assist board members to make an informed judgment on whether the bank is managing its compliance risk effectively; and
 - (c) report promptly to the board of directors or a committee of the board 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).

- 2.4 Senior management must take the necessary measures to ensure that the bank can rely on a permanent and effective compliance function that is consistent with the following principles.

III. COMPLIANCE FUNCTION PRINCIPLES

A. INDEPENDENCE

Principle

3. The bank's compliance function must be independent.

Guidelines

- 3.1 The concept of independence involves four related elements, each of which is considered in more detail below.
- 3.1.1 First, the compliance function must have a formal status within the bank.
- 3.1.2 Second, there must be a group compliance officer or head of compliance with overall responsibility for co-ordinating the management of the bank's compliance risk.
- 3.1.3 Third, compliance function staff, and in particular, the head of compliance, must not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have.
- 3.1.4 Fourth, compliance function staff must have access to the information and personnel necessary to carry out their responsibilities.
- 3.2 The concept of independence does not mean that the compliance function cannot work closely with management and staff in the various business units. A co-operative working relationship between compliance function and business units must help to identify and manage compliance risks at an early stage. Rather, the various elements described below must be viewed as safeguards to help ensure the effectiveness of the compliance function, notwithstanding the close working relationship between the compliance function and the business units. The way in which the safeguards are implemented will depend to some extent on the specific responsibilities of individual compliance function staff.

Status

- 3.3 The compliance function must have a formal status within the bank to give it the appropriate standing, authority and independence. This may be set out in the bank's compliance policy or in any other formal document. The document must be communicated to all staff throughout the bank.

- 3.4 The following issues with respect to the compliance function must be addressed in the document:
- (a) its role and responsibilities;
 - (b) measures to ensure its independence;
 - (c) its relationship with the internal audit function and other risk management functions within the bank;
 - (d) in cases where compliance responsibilities are carried out by staff in different departments, how these responsibilities are to be allocated among the departments;
 - (e) its right to obtain access to information necessary to carry out its responsibilities, and the corresponding duty of bank staff to co-operate in supplying this information;
 - (f) its right to conduct investigations of possible breaches of the compliance policy and to appoint outside experts to perform this task if appropriate;
 - (g) its right to be able freely to express and disclose its findings to senior management, and if necessary, the board of directors or a committee of the board;
 - (h) its formal reporting obligations to senior management; and
 - (i) its right of direct access to the board of directors or a committee of the board.

Head of Compliance

- 3.5 Each bank must have an executive or senior staff member with overall responsibility for co-ordinating the identification and management of the bank's compliance risk and for supervising the activities of other compliance function staff, referred to herein by the title "head of compliance" to describe this position.
- 3.6 The nature of the reporting line or other functional relationship between staff exercising compliance responsibilities and the head of compliance will depend on how the bank has chosen to organise its compliance function. Compliance function staff who reside in operating business units or in local subsidiaries may have a reporting line to operating business unit management or local management. This is not objectionable, provided such staff also have a reporting line through to the head of compliance as regards their compliance responsibilities. In cases where compliance function staff reside in independent support units (e.g. legal, financial control, risk management), a separate reporting line from staff in these units to the head of compliance may not be necessary. However, these units must co-operate closely with the head of compliance to ensure that the head of compliance can perform his or her responsibilities effectively.

- 3.7 The head of compliance must normally be a member of senior management. If the head of compliance is a member of senior management, he or she must not have direct business line responsibilities. If the head of compliance is not a member of senior management, he or she must have a direct reporting line to a member of senior management who does not have direct business line responsibilities.
- 3.8 The AMBD and the board of directors must be informed when the head of compliance takes up or leaves that position and, if the head of compliance is leaving the position, the reasons for his or her departure. For branches of foreign banks in Brunei, the AMBD must be promptly informed of the arrival or departure of the local head of compliance.

Conflicts of interest

- 3.9 The independence of the head of compliance and any other staff having compliance responsibilities may be undermined if they are placed in a position where there is a real or potential conflict between their compliance responsibilities and their other responsibilities. It is preferable that compliance function staff perform only compliance responsibilities. The AMBD recognises, however, that this may not be practicable in the case of smaller branches of foreign banks in Brunei. In these cases, therefore, compliance function staff may perform non-compliance tasks, provided potential conflicts of interest are avoided.
- 3.10 The independence of compliance function staff may also be undermined if their remuneration is related to the financial performance of the business line for which they exercise compliance responsibilities. However, remuneration related to the financial performance of the bank as a whole should generally be acceptable.

Access to information and personnel

- 3.11 The compliance function must have the right on its own initiative to communicate with any staff member and obtain access to any records or files necessary to enable it to carry out its responsibilities.
- 3.12 The compliance function must be able to carry out its responsibilities on its own initiative in all departments of the bank in which compliance risk exists. It must have the right to conduct investigations of possible breaches of the compliance policy and to request assistance from specialists within the bank (e.g. legal or internal audit) or engage outside specialists to perform this task if appropriate.

- 3.13 The compliance function must be free to report to senior management on any irregularities or possible breaches disclosed by its investigations, without fear of retaliation or disfavour from management or other staff members. Although its normal reporting line must be to senior management, the compliance function must also have the right of direct access to the board of directors or to a committee of the board, bypassing normal reporting lines, when this appears necessary. Further, the audit committee must meet with the head of compliance at least annually, as this will help it to assess the extent to which the bank is managing its compliance risk effectively.

B. RESOURCES

Principle

4. The bank's compliance function must have the resources to carry out its responsibilities effectively.

Guidelines

- 4.1 The resources of the compliance function must be both sufficient and appropriate to ensure that compliance risk within the bank is managed effectively. In particular, compliance function staff must have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their specific duties. Compliance function staff must have a sound understanding of compliance laws, rules and standards and their impact on the bank's operations. The professional skills of compliance function staff, especially keeping up-to-date with developments in compliance laws, rules and standards, must be maintained through regular and systematic education and training.

C. COMPLIANCE FUNCTION RESPONSIBILITIES

Principle

5. The responsibilities of the bank's compliance function must be to assist senior management in managing effectively the compliance risks faced by the bank. 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 must be clear.

Guidelines

- 5.1 Not all compliance responsibilities are necessarily carried out by the "compliance function". Compliance responsibilities may be exercised by staff in different departments. In some banks, legal and compliance may be separate departments; the legal department may be responsible for advising management on the compliance laws, rules and standards and for preparing guidance to staff, while the compliance department may be responsible for monitoring compliance with the policies and procedures and reporting to management. In other banks, parts of the compliance function may be located within the operational risk group. If there is a division of responsibilities between departments, the allocation of responsibilities to each department must be clear. There must also be appropriate mechanisms for co-operation among each department and with the head of compliance (e.g. with respect to the provision and exchange of relevant advice and information). These mechanisms must be sufficient to ensure that the head of compliance can perform his or her responsibilities effectively.

Advice, guidance and education

- 5.2 The compliance function must advise senior management on compliance laws, rules and standards, including keeping them informed on developments in the area.
- 5.3 The compliance function must assist senior management in:
- (a) educating staff on compliance issues, and acting as a contact point within the bank for compliance queries from staff members; and
 - (b) establishing written guidance to staff on the appropriate implementation of compliance laws, rules and standards through policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.

Identification, measurement and assessment of compliance risk

- 5.4 The compliance function must, on a pro-active basis, identify, document and assess the compliance risks associated with the bank's business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships. If the bank has a new products committee, compliance function staff must be represented on the committee.
- 5.5 The compliance function must also consider ways to measure compliance risk (e.g. by using performance indicators) and use such measurements to enhance compliance risk assessment. Technology can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems (e.g. an increasing number of customer complaints, irregular trading or payments activity, etc).
- 5.6 The compliance function must assess the appropriateness of the bank's compliance procedures and guidelines, promptly follow up any identified deficiencies, and, where necessary, formulate proposals for amendments.

Monitoring, testing and reporting

- 5.7 The compliance function must monitor and test compliance by performing sufficient and representative compliance testing. The results of the compliance testing must be reported to senior management in accordance with the bank's internal risk management procedures.
- 5.8 The head of compliance must report on a regular basis to senior management on compliance matters. The reports must refer to the compliance risk assessment that has taken place during the reporting period, including any changes in the compliance risk profile based on relevant measurements such as performance indicators, summarise any identified breaches and/or deficiencies and the corrective measures recommended to address them, and report on corrective measures already taken. The reporting format must be commensurate with the bank's compliance risk profile and activities.

Statutory responsibilities and liaison

- 5.9 The compliance function may have specific statutory responsibilities (e.g. fulfilling the role of anti-money laundering officer). It may also liaise with relevant external bodies, including regulators, standard setters and external experts.

Compliance programme

- 5.10 The responsibilities of the compliance function must be carried out under a compliance programme that sets out its planned activities, such as the implementation and review of specific policies and procedures, compliance risk assessment, compliance testing and educating staff on compliance matters. The compliance programme must be risk-based and subject to oversight by the head of compliance to ensure appropriate coverage across businesses and co-ordination among risk management functions.

D. RELATIONSHIP WITH INTERNAL AUDIT

Principle

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

Guidelines

- 6.1 Compliance risk must be included in the risk assessment methodology of the internal audit function, and the internal audit programme must cover the adequacy and effectiveness of the bank's compliance function, including testing of controls commensurate with the perceived level of risk.
- 6.2 This principle requires that the compliance function and the audit function must be separate, to ensure that the activities of the compliance function are subject to independent review. It is important, therefore, that there is a clear understanding within the bank as to how risk assessment and testing activities are divided between the two functions, and that this is documented (e.g. in the bank's compliance policy or in a related document such as a protocol). The internal audit function must, of course, keep the head of compliance informed of any audit findings relating to compliance.

IV. OTHER MATTERS

A. CROSS-BORDER ISSUES

Principle

7. Banks must comply with applicable laws and regulations in all jurisdictions in which they conduct business, and the structure of the compliance function must be consistent with local legal and regulatory requirements.

Guidelines

- 7.1 Banks which conduct business internationally through local subsidiaries or branches, or in other jurisdictions where they do not have a physical presence must comply with local laws and regulations. Banks must ensure that compliance responsibilities specific to each jurisdiction are carried out by individuals with the appropriate local knowledge and expertise, with oversight from the head of compliance in co-operation with the bank's other risk management functions.
- 7.2 The bank must put procedures in place to identify and assess the possible increased reputational risk to the bank if it offers products or carries out activities in certain jurisdictions that would not be permitted in its home jurisdiction.

B. OUTSOURCING

Principle

8. Compliance must be regarded as a core risk management activity within the bank. Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the head of compliance.

Guidelines

- 8.1 Banks must follow the AMBD Guidelines on outsourcing. Banks must ensure that any outsourcing arrangements do not impede effective supervision by the AMBD. If any component of the compliance function is outsourced, the board of directors and senior management remain responsible for compliance by the bank with all applicable laws, rules and standards.

- END -