



MODULE	HC:	High-Level Controls
CHAPTER	HC-6:	Management Structure

HC-6.4 Compliance

HC-6.4.1 Compliance starts at the top. It will be most effective in a corporate culture that emphasises standards of honesty and integrity and in which the board of directors and senior management lead by example. It concerns everyone within the bank and should be viewed as an integral part of the bank's business activities. A bank should hold itself to high standards when carrying on business, and at all times strive to observe the spirit as well as the letter of the law. Failure to consider the impact of its actions on its shareholders, customers, employees and the markets may result in significant adverse publicity and reputational damage, even if no law has been broken.

HC-6.4.2 **Islamic bank licensees must establish an effective compliance framework, which is appropriate for the size and complexity of their operations, for managing their compliance risks.**

HC-6.4.3 The term "Compliance risk" refers to the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, directives, directions, reporting requirements and codes of conduct, including internal code of conduct.

HC-6.4.4 Compliance laws, rules and standards generally cover matters such as observing proper prudential standards, standards of market conduct, managing conflicts of interest, treating customers fairly and ensuring suitability of customer advice, as well as matters specified in HC-6.4.3 above. They typically include specific areas such as the prevention of money laundering and terrorist financing, and may extend to tax laws that are relevant to the structuring of banking products or customer advice.

HC-6.4.5 It is important that banks do not consider compliance function as a cost center rather it is an activity that enhances the reputation of the bank and promotes the right environment for better financial performance.

HC-6.4.6 The relationship between a bank's business units, the support functions and the compliance function can be explained using the three lines of defence model.

- a) The business units are the first line of defence. They undertake the management of risks within assigned limits of risk exposure and are responsible and accountable for identifying, assessing and controlling the risks of their business.
- b) The second line of defence includes the support functions, such as risk management, compliance, legal, human resources, finance, operations, and technology. Each of these functions, in close relationship with the business units, ensures that risks in the business units have been appropriately identified and managed. The business support functions work closely to help define strategy, implement bank policies and procedures, and collect information to create a bank-wide view of risks.
- c) The third line of defence is the internal audit function that independently assesses the effectiveness of the controls over the processes created in the first and second lines of defence and provides assurance on these processes. The responsibility for internal control does not transfer from one line of defence to the next line.



MODULE	HC: High-Level Controls
CHAPTER	HC-6: Management Structure

HC-6.4 Compliance (continued)

Responsibilities of the Board of Directors

HC-6.4.7

The board of directors of an Islamic bank licensee is responsible for overseeing the management of the bank's compliance risk. The board must establish a permanent and effective compliance function and approve the bank's compliance policies and procedures for identifying, assessing, monitoring, reporting and advising on compliance risk. At least once a year, the board or a designated board committee must assess the extent to which the bank is managing its compliance risk effectively. The board must also ensure that the agenda for the meetings of the board or the designated board committee include compliance as a topic at least every quarter.

HC-6.4.8

The board designated committee referred to in HC-6.4.7 may be the audit committee, the governance committee, the risk committee, or other committee which does not have a role in the business or executive roles, such as those relevant to executive committees and investment committees. For branches of foreign bank licensees, all references in this Section to the Board/the designated board committee should be interpreted as the Group Compliance Officer or a sufficiently senior level Regional Compliance Committee or Officer.

Responsibilities of the Senior Management

HC-6.4.9

Senior management is responsible for effective management of bank's compliance risk.

HC-6.4.10

Senior management is responsible for establishing the operating framework and the processes to support a permanent and an effective compliance function. It is responsible for establishing and communicating a written compliance policy through all levels of the organisation for ensuring that it is adhered to in practice.



MODULE	HC: High-Level Controls
CHAPTER	HC-6: Management Structure

HC-6.4 Compliance (continued)

- HC-6.4.11** The compliance policy must be approved by the Board/the designated board committee and must address the following:
- (a) The role and responsibilities of the compliance function;
 - (b) Measures to ensure its independence;
 - (c) Its relationship with other risk management functions within the bank and with the internal audit function;
 - (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 relevant laws and regulations and the compliance policy and to appoint outside experts to perform this task if appropriate; and
 - (g) Its right to be able freely to express and disclose its findings to the board of directors or to the designated board committee, e.g. the audit committee or the governance committee of the board.
 - (h) The basic principles to be followed by management and staff describing the main processes by which compliance risks are to be identified and managed through all levels of the organization.

- HC-6.4.12** The Board and the designated Board committee must ensure that all compliance findings and recommendations are resolved within six months for high risk/critical issues and 9 months for any other issues from the issue date of the subject compliance report unless otherwise agreed with the CBB taking into consideration time required for specific issues that may require substantive changes to technology, systems and/or processes.



MODULE	HC: High-Level Controls
CHAPTER	HC-6: Management Structure

HC-6.4 Compliance (continued)

HC-6.4.13

Senior management must assess the training needs of staff taking into account the existing skills and competencies, the nature of changes to laws and regulations in developing a training plan for compliance across all levels throughout the organisation. Training must be provided by competent and skilled personnel, whether available internally or externally. Training that is provided must reflect the seniority, role and responsibilities of the individuals for whom it is intended.

Compliance Function

HC 6.4.14

Islamic bank licensees must organise their compliance function and set priorities for the management of their compliance risk in a way that is consistent with their own risk management strategy and structures.

HC-6.4.15

The compliance function must be independent and effective. It must be headed by 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.

HC-6.4.16

The Head of Compliance, with the assistance of senior management must:

- (a) report to the board of directors or the designated committee of the board on a quarterly basis, even if there are no issues to highlight,
- (b) report to the board or the designated 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;
- (c) report promptly to the board or the designated committee of the board on any material compliance failures as they arise (e.g. failures that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation); and
- (d) ensure that senior management develop remedial action plans to address compliance breaches.

HC-6.4.17

The role of head of compliance may be combined with those of the head of risk if the size and nature of the bank justifies a single function for both roles. Banks which carry out limited operations or are small branches of foreign banks would qualify for such a practice.



MODULE	HC: High-Level Controls
CHAPTER	HC-6: Management Structure

HC-6.4 Compliance (continued)

HC-6.4.18 The compliance function should assist senior management, the board and the designated committee of the board in their compliance obligations and help promote the right culture within the bank. While the board and management are accountable for the bank's compliance, the compliance function has an important role in supporting corporate values, policies and processes that help ensure that the bank acts responsibly and fulfils all applicable obligations.

HC-6.4.19

The independence and effectiveness of the function must be based on the following related elements:

- (a) The compliance function must have a formal status with sufficient authority within the bank;
- (b) 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;
- (c) 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 have;
- (d) Compliance function staff must have access to the information and personnel necessary to carry out their responsibilities; and
- (e) The compliance function must directly report to the board or a designated board committee in the case of Bahraini Islamic bank licensees and administratively to the CEO; and
- (f) In the case of branches of foreign bank licensees, the reporting must be to the Group Compliance Officer or Regional Compliance Officer and may report administratively to the CEO/GM.

HC-6.4.20 The concept of independence does not mean that the compliance function cannot work closely with management and staff in the various business units. Indeed, a co-operative working relationship between compliance function and business units should help to identify and manage compliance risks at an early stage. Rather, the various elements described above should 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.

HC-6.4.21 The compliance function should be free to highlight 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.



MODULE	HC: High-Level Controls
CHAPTER	HC-6: Management Structure

HC-6.4 Compliance (continued)

HC-6.4.22 Appointment, dismissal and other changes to the head of compliance must be approved by the board or the designated board committee. Appointments of head of compliance must be approved by the CBB in accordance with paragraph LR-IA.1.17. If the head of compliance is removed from his or her position for any reason, this must be notified to the CBB, describing fully the reasons as required under paragraph LR-1A.1.22.

HC-6.4.23 Islamic bank licensees must ensure that the compliance risk management framework is subject to an independent review by a third party consultant, other than the external auditor, every three years and when there are material changes to the business. The results of the independent review and action must be provided to the CBB by 30th September of the relevant year.

HC-6.4.24 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.

HC-6.4.25 The Compliance function must on a pro-active basis, identify, measure, 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, the compliance function staff should be represented on the committee.

HC-6.4.26 While the Compliance function is responsible for oversight and compliance checks across the full spectrum of compliance risk areas, it is recognised that many areas of compliance require specialist skills which can be found in different parts of the organisation, example, the skill sets for compliance with ICAAP can be found either with financial control or with risk management, for compliance with labour laws, the specialist skills are with human resources departments etc. In such cases, the compliance function ensures that the right levels of checks and balances and compliance reporting are available to get comfort that the licensee has adhered to the relevant requirements. In certain instances, it may use external experts with the approval of the relevant authority within the bank.



MODULE	HC: High-Level Controls
CHAPTER	HC-6: Management Structure

HC-6.4 Compliance (continued)

HC-6.4.27 The compliance function should consider ways to measure compliance risk (e.g. by using performance indicators) and use such measurements to enhance compliance risk assessment.

HC-6.4.28 In case of new regulations, 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

HC-6.4.29 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 the Audit Committee.

HC-6.4.30 The compliance function must advise senior management and the designated committee of the board on all relevant laws, rules and standards, in all jurisdictions in which the bank conducts its business, and inform them on developments in the subject.

Guidance and education

HC-6.4.31 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 laws, rules and standards through policies and procedures and other documents such as manuals, internal codes of conduct and practice guidelines.

Statutory responsibilities and liaison

HC-6.4.32 The compliance function must 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.



MODULE	HC:	High-Level Controls
CHAPTER	HC-6:	Management Structure

HC-6.4 Compliance (continued)

Right of access

HC-6.4.33

The compliance function must have access across the entire organisation to carry out its responsibilities on its own initiative where compliance risk exists. It must, additionally, have the right to communicate with any staff member and to obtain access to any records or files necessary to conduct its responsibilities and 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' subject to appropriate internal approval to perform this task if appropriate.

Competent Resources

HC-6.4.34

The compliance function must have adequate resources to carry out its functions effectively commensurate with the size and complexity of the organisation. The resources to be provided for the compliance function must be both sufficient and appropriate to ensure that compliance risk within the bank is managed effectively.

HC-6.4.35

The 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 laws, rules and standards and their practical impact on the bank's operations.

HC-6.4.36

The professional skills of compliance function staff, especially with respect to keeping up-to-date with developments in compliance laws, rules and standards, must be maintained through regular and systematic education and training.

Relationship with Internal Audit

HC-6.4.37

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

HC-6.4.38

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 bank's compliance function should be established, including testing of controls commensurate with the perceived level of risk.



MODULE	HC: High-Level Controls
CHAPTER	HC-6: Management Structure

HC-6.4 Compliance (continued)

HC-6.4.39

The compliance function and the internal 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.

Cross-border Issues

HC-6.4.40

Islamic bank licensees that conduct business through a branch or subsidiary in other jurisdictions must through the Group Compliance Function:

- (a) comply with local laws and regulations;
- (b) have Group Compliance policy and procedures; and
- (c) conduct annual compliance testing on overseas operations whose total revenue represents 20% or more of the Group's total revenue and on every two years' basis for other overseas operations.

HC-6.4.41

Islamic bank licensees must have 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.

HC-6.4.42

Islamic bank licensees with overseas operations must establish a Group Compliance Function which must oversee the compliance activities on a group-wide basis. The Group Compliance Officer must ensure that compliance reviews and checks are carried out at branches and subsidiaries. As legal and regulatory requirements may differ from jurisdiction to jurisdiction, compliance issues specific to each jurisdiction must be coordinated within the structure of the bank's group-wide compliance policy.

HC-6.4.43

The senior management with assistance of Group Compliance Officer must ensure that adequate resources, commensurate with the scale and complexity of the operations, are assigned for compliance activities at, the head office, branches and subsidiaries.



MODULE	HC: High-Level Controls
CHAPTER	HC-6: Management Structure

HC-6.4 Compliance (continued)

HC-6.4.44

The Group Compliance Officer must ensure that adequate reports and information is received from overseas branches and subsidiaries on compliance related issues.

Outsourcing

HC-6.4.45

Compliance function or its activities must not be outsourced.

Other requirements

HC-6.4.46

Every application/request for approval to the CBB must be accompanied by a compliance assessment report confirming that all related requirements pertaining to the request have been thoroughly checked by the compliance function including the impact of such a request on the licensee's financial position and compliance status. In addition, reference must be made to any previously approved arrangements by the CBB.

HC6.4.47

In cases where the requests have a potential financial impact on the licensee a report from the financial control function in consultation with external auditors must also be submitted as part of the compliance assessment report, whereas in case of any legal implication of such a request a legal opinion on the matter must be submitted.

HC-6.4.48

Where breaches or deficiencies have occurred due to failures by approved persons, the CBB may consider re-assessing the fitness and propriety of such persons.