هيئة تنظيم مركز قطر للمال

QATAR FINANCIAL CENTRE
REGULATORY AUTHORITY

Governance and Controlled Functions Rules 2020 (CTRL)

Version No. 1

Effective: 1 July 2021

هيئة تنظيم مركز قطر للمال
QATAR FINANCIAL CENTRE
REGULATORY AUTHORITY

Governance and Controlled Functions Rules 2020

QFCRA Rules 2020-4

made under the

Financial Services Regulations

Contents

Chapter 1 General

Part 1.1 Preliminary

1.1.1 Name of rules

These rules are the *Governance and Controlled Functions Rules 2020* (or ***CTRL***).

1.1.2 Commencement

These rules commence on 1 July 2021.

1.1.3 Effect of definitions, notes and examples

(1) A definition in the Glossary also applies to any instructions or document made under these rules.

(2) A note in or to these rules is explanatory and is not part of these rules. However, examples and guidance are part of these rules.

(3) An example is not exhaustive, and may extend, but does not limit, the meaning of these rules or the particular provision of these rules to which it relates.

Note Under FSR, article 17 (4), guidance is indicative of the view of the Regulatory Authority at the time and in the circumstances in which it was given.

1.1.4 Application of CTRL

(1) These rules apply to an authorised firm in relation to the carrying on of a regulated activity in or from the QFC.

(2) These rules also apply to:

(a) an authorised firm's governance, its risk management framework, and its policies and procedures, outside the QFC to the extent that they relate to a regulated activity carried on in or from the QFC; and

(b) every function exercised by or on behalf of an authorised firm outside the QFC (including any outsourced function), to the extent that the function relates to the carrying on of a regulated activity in or from the QFC.

Part 1.2 Key concepts

Division 1.2.A Key concepts — corporate governance

1.2.1 What is a firm's *governing body*?

For these rules, an authorised firm's ***governing body*** is:

(a) in the case of a firm that is incorporated as a company or a limited liability partnership in the QFC, or is a partnership constituted under the *Partnership Regulations 2007* — its board of directors or the body (whatever it is called) that, under the firm's constitutional document, has the responsibility of overseeing the firm's business in or from the QFC; and

(b) in the case of a firm that is a branch:

(i) the firm's board of directors, or a committee of that board, that has the responsibility of overseeing the firm's business in or from the QFC; or

(ii) that part of the firm's committee of management or other body (whatever it is called) that has the responsibility of overseeing the firm's business in or from the QFC.

Guidance

This definition draws a distinction (for some purposes) between:

- a firm that is incorporated or formed in the QFC; and
- a firm that is incorporated or formed outside the QFC (that is, a branch).

In the case of a branch, the firm's board (wherever it is located) remains ultimately responsible for the oversight of the firm, but many policy decisions may be made by a part, or a delegate, of the firm's board. These rules recognise that firms choose to allocate their responsibilities and undertake their business in different ways; these rules therefore place the responsibility for certain kinds of oversight on the firm's board or the part or delegate of the board.

1.2.2 What is a firm's *corporate governance framework*?

(1) An authorised firm's ***corporate governance framework*** is made up of the firm's organisational structures, policies, procedures and

systems and controls as they relate to the firm's business objectives and the means of achieving them.

(2) An authorised firm's corporate governance framework includes:

(a) the firm's risk management framework (see rule 1.2.3);

(b) its internal control and assurance functions (that is, its risk management, compliance oversight, internal audit and actuarial functions);

(c) its business objectives; and

(d) the corporate governance obligations in these rules, the Companies Regulations, and other applicable regulations, rules and guidance.

Guidance

1 The corporate governance framework deals with the relationships between a firm's board, its senior management, depositors, policyholders, clients and other stakeholders. Other important aspects of corporate governance are the separation of functions within the firm and the accountabilities for the internal control and assurance functions.

2 The corporate governance framework includes at least the firm's objectives and the firm's corporate governance obligations under these rules, the Companies Regulations, and other regulations, rules and guidance.

1.2.3 What is a firm's *risk management framework*?

(1) An authorised firm's governing body must establish a risk management framework.

Note For the firm's risk management framework, see rule 7.1.2.

(2) The firm's ***risk management framework*** is made up of:

(a) the firm's systems for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating risks that may affect the firm's ability to meet its obligations; and

(b) the structures, policies, processes and people that support those systems.

1.2.4 What is a firm's *internal controls and assurance framework*?

(1) An authorised firm's governing body must establish an ***internal controls and assurance framework*** made up of the firm's internal control and assurance functions.

Note In relation to an authorised firm's internal controls and assurance framework, see Chapter 6.

(2) The following controlled functions are the ***internal control and assurance functions***:

(a) the risk management function (see rule 1.2.12);

(b) the compliance oversight function (see rule 1.2.13);

(c) the internal audit function (see rule 1.2.14);

(d) the actuarial function (see rule 1.2.15).

(3) The internal controls and assurance framework must provide reasonable assurance on the effectiveness and efficiency of the firm's operations, the reliability of its financial reporting and the extent of its compliance with applicable laws and regulations.

Division 1.2.B Key concepts—controlled functions

1.2.5 What are *controlled functions*?

(1) FSR, article 41, requires that, to exercise a controlled function for an authorised firm, an individual must be an approved individual, and authorises the Regulatory Authority to specify, in rules, the functions that are controlled functions.

Note The assessment, training and competency of individuals to exercise controlled functions is dealt with in INDI.

(2) For FSR, article 41 (2), each of the following is a ***controlled function***:

(a) the non-executive governance function;

(b) the executive governance function;

(c) the senior executive function;

(d) the finance function;

(e) the senior management function;

(f) the MLRO function;

(g) the risk management function;

(h) the compliance oversight function;

(i) the internal audit function;

(j) the actuarial function.

Note 1 Each of the controlled functions mentioned in subrule (2) (other than the MLRO function) is described elsewhere in these rules. There are signpost definitions in the Glossary.

Note 2 The non-executive governance function, the executive governance function, the senior executive function, the finance function and the senior management function are responsible for the firm's governance and general management — see Chapter 3.

Note 3 The MLRO function is to do with compliance and reporting under the law relating to money laundering and preventing the financing of terrorism — see AML/CFTR or (for general insurance firms only) AMLG. The MLRO function is not further dealt with in these rules.

Note 4 The matters referred to in FSR, article 41 (3) (application for approval as an approved individual, principles to be adhered to by approved individuals, reporting by approved individuals and withdrawal of authorisation) are set out in INDI.

1.2.6 What is the *executive governance function*?

(1) The ***executive governance function*** for an authorised firm that is a QFC entity is the function of being a member (other than a non-executive member) of the firm's governing body.

(2) The ***executive governance function*** for an authorised firm that is a branch is the function of being a member of the firm's governing body with responsibility for the firm's business in or from the QFC.

1.2.7 What is the *non-executive governance function*?

The ***non-executive governance function*** for an authorised firm that is a QFC entity is the function of being a member of the firm's governing body but not being responsible for the day-to-day direction of the firm's affairs.

1.2.8 What is the *senior executive function*?

The ***senior executive function*** for an authorised firm is the function of being responsible for:

(a) the whole business of the firm; or

(b) in the case of an authorised firm that is a branch — the business of the firm carried on in or from the QFC.

1.2.9 What is the *finance function*?

The ***finance function*** for an authorised firm includes the functions of being responsible for the prudential returns that the firm is required to prepare, and ensuring that the firm's financial records are accurate and complete.

1.2.10 What is the *senior management function*?

The ***senior management function*** for an authorised firm is the function of being responsible (alone or with others) for managing and supervising a part or parts of the firm's business related to its regulated activities (other than parts that are included in any of the other controlled functions).

1.2.11 What is the *MLRO function*?

The ***MLRO function*** for an authorised firm is the function of being the firm's MLRO under either AML/CFTR or AMLG.

Note The MLRO function is not dealt with further in these rules. For firms' obligations in relation to the MLRO function see:

- for general insurance firms — AMLG
- for all other authorised firms — AML/CFTR.

1.2.12 What is the *risk management function*?

The ***risk management function*** for an authorised firm is the function of being responsible for:

(a) the firm's risk management framework; and

(b) overseeing and reviewing the firm's implementation of, and its compliance with, those policies, procedures and controls.

Note For more on the risk management function, see Part 6.2; for risk management generally, see Chapter 7.

1.2.13 What is the *compliance oversight function*?

The ***compliance oversight function*** for an authorised firm is the function of being responsible for:

(a) the firm's compliance policies, procedures and controls; and

(b) overseeing and reviewing the firm's implementation of, and its compliance with, those policies, procedures and controls.

Note For more on the compliance oversight function, see Part 6.3.

1.2.14 What is the *internal audit function*?

The ***internal audit function*** for an authorised firm is the function of being responsible for:

(a) the firm's internal audit policies, procedures and controls; and

(b) overseeing and reviewing the firm's implementation of, and its compliance with, those policies, procedures and controls.

Note For more on the internal audit function, see Part 6.4.

1.2.15 What is the *actuarial function*?

The ***actuarial function*** for an authorised firm is the function of being responsible for:

(a) the firm's actuarial policies, procedures and controls; and

(b) overseeing and reviewing the firm's implementation of, and its compliance with, those policies, procedures and controls.

Note For more on the actuarial function, see Part 6.5.

Chapter 2 Corporate governance principles

2.1.1 Principle 1 — approval of corporate governance framework

The governing body of an authorised firm must approve a corporate governance framework for the firm:

(a) that is appropriate to the nature, scale and complexity of the firm's business; and

(b) under which the governing body is ultimately responsible for ensuring that the firm carries out the firm's obligations under these rules.

2.1.2 Principle 2 — implementation of corporate governance framework

The senior management of an authorised firm must ensure that the corporate governance framework is effectively implemented and maintained throughout the firm's business.

2.1.3 Principle 3 — knowledge, skills and expertise

The governing body and senior management of an authorised firm must have an appropriate mix of knowledge, skills and expertise to ensure that the firm is effectively managed commensurately with the nature, scale and complexity of its business.

2.1.4 Principle 4 — review

The governing body of an authorised firm must ensure that the firm reviews its corporate governance framework and risk management framework appropriately, and does so sufficiently often to ensure that:

(a) the frameworks remain effective;

(b) the functions within the frameworks remain independent; and

(c) any necessary corrective action is taken.

Note The review must be carried out every 3 years, or more often if the Regulatory Authority so directs—see rule 3.1.19.

2.1.5 Principle 5 — transparency

(1) The governing body of an authorised firm that is a company must disclose to the firm's shareholders, customers and other stakeholders the information necessary to enable them to assess the effectiveness of the governing body and senior management in governing and managing the firm.

(2) The firm must disclose at least the following:

(a) the names of the members of the body and its committees;

(b) information on the firm's objectives, its organisational and governance structures and policies, and its major shareholders.

(3) The extent of the disclosure must be proportionate to the firm's size, complexity, structure, economic significance and risk profile.

(4) The firm may comply with this rule by publishing the information on its website.

Chapter 3 Governing bodies

Note for Chapter 3

The Parts of this Chapter apply to authorised firms as follows:

- Part 3.1 applies to all authorised firms
- Part 3.2 applies only to authorised firms that are branches
- Part 3.3 applies only to authorised firms that are incorporated in the QFC
- Part 3.4 applies to all authorised firms, except for rule 3.4.1 (4)) which applies only to firms that are incorporated in the QFC.

Part 3.1 Governing bodies — all authorised firms

Division 3.1.A Application of Part 3.1

3.1.1 Application of Part 3.1

This Part applies to all authorised firms.

Division 3.1.B Governing bodies — membership

3.1.2 Members of governing body to be approved individuals

A member of an authorised firm's governing body must be an individual who is approved to exercise the appropriate controlled function, as follows:

(a) for an executive member — the executive governance function;

(b) for a non-executive member — the non-executive governance function.

3.1.3 What individuals are eligible as independent non-executive member?

(1) An individual is eligible to be an independent non-executive member of the governing body of an authorised firm unless:

(a) he or she is, or has been during the last 3 years:

(i) an employee of the firm; or

(ii) an employee, board member, owner, partner or controller of a consultant to the firm (including the firm's external auditor);

(b) he or she is a relative of a member of the firm's senior management;

(c) within the last 3 years, he or she or any of his or her relatives has had, directly or indirectly, 1 or more substantial commercial or financial transactions with the firm;

(d) he or she is receiving, or has received during the last 3 years, remuneration from the firm (other than as a member of its governing body);

(e) he or she:

(i) owns 1% or more of the shares of the firm; or

(ii) is a representative of a legal person that owns 5% or more of the shares of the firm or another company in its corporate group;

(f) he or she has been a member of the firm's governing body for longer than 9 consecutive years; or

(g) he or she might reasonably be taken to have a conflict of interest because of a personal or business relationship with:

(i) a member of the firm's governing body, the individual who exercises the senior executive function for the firm, or a member of the firm's senior management; or

(ii) a major shareholder of the firm.

Division 3.1.C Governing bodies — role and obligations

3.1.4 Governing body's general role

An authorised firm's governing body has overall responsibility for the firm. That responsibility includes approving and overseeing the implementation of the firm's strategic objectives, corporate governance framework and corporate culture.

3.1.5 Governing body's obligations not to be repudiated

A governing body cannot relieve itself of an obligation under this Division by repudiating the obligation or allocating it to another person or body.

3.1.6 Allocation of responsibilities

(1) The governing body of an authorised firm retains primary responsibility for all of the firm's operations at all times. The firm's senior management is responsible for effectively implementing the governing body's business strategy consistently with the governing body's policies and risk appetite and under the governing body's supervision.

(2) The governing body must give the individual who exercises the senior executive function for the firm a written document that sets out his or her responsibilities. The individual must acknowledge, in writing, having received that document, and must confirm in the acknowledgement that he or she understands, and undertakes to carry out, those responsibilities.

(3) Unless the governing body specifically allocates a responsibility, it retains it.

(4) The individual who exercises the firm's senior executive function must give each individual who exercises a controlled function for the firm a written document that sets out that individual's responsibilities.

(5) The individual who exercises the firm's senior executive function must obtain the governing body's approval (or the approval of the body's audit committee, if any) of the content of the document given to the individual who exercises the internal audit function.

(6) The individual who exercises the firm's senior executive function must consult with the governing body (or the body's risk committee, if any) in relation to the content of the document given to the individual who exercises the risk management function.

(7) The individual who exercises the firm's senior executive function must not attempt, in a document referred to in subrule (4), to restrict,

limit or compromise any right, duty, responsibility or authority conferred by these rules or any other Rules on an individual who exercises any other controlled function.

(8) Each such individual must acknowledge, in writing, having received that document, and must confirm in the acknowledgement that he or she understands, and undertakes to carry out, those responsibilities.

(9) Unless the individual who exercises the senior executive function specifically allocates a responsibility, he or she retains it.

(10) The allocation of a responsibility by the governing body does not remove or reduce the body's duty to oversee the individual who exercises the firm's senior executive function and the firm's senior management. Also, the allocation of a responsibility by the individual who exercises the senior executive function does not remove or reduce the individual's duty to exercise oversight in relation to the other controlled functions.

(11) The scope of the responsibilities allocated to an individual who exercises a controlled function for the firm must not be less than the scope of the controlled function as set out in these rules and INDI.

(12) The allocation of responsibilities referred to in this rule is separate from operational authorities and limits exercised by the individual who exercises the firm's senior executive function and the firm's senior management (such as limits on loan approvals, underwriting, claims handling, investments, or signing cheques).

(13) The governing body:

(a) must ensure that the firm's business can be adequately managed by the body, the individual who exercises the firm's senior executive function and the firm's senior management; and

(b) must consider whether the firm's senior management (other than the individual who exercises the senior executive function, and the individual who exercises the risk management function for a QFC insurer) ought to be ordinarily resident in Qatar to exercise their functions properly.

Note The individual who exercises the senior executive function for an authorised firm, and the individual who exercises the risk management function for a QFC insurer, are already required by these rules to be ordinarily resident in Qatar — see respectively rules 4.1.4 (2) and 6.2.3 (4) (b).

3.1.7 General obligations — decision-making

An authorised firm's governing body:

(a) must ensure that it has access to sufficient information and independent advice about the firm's affairs to make informed decisions and discharge its responsibilities effectively; and

(b) must be mindful of the legitimate interests of shareholders, customers and other stakeholders when making decisions.

3.1.8 General obligations — engagement

An authorised firm's governing body:

(a) must keep up with material changes in the firm's business and external environment; and

(b) must act in a timely manner to protect the firm's long-term interests.

3.1.9 General obligations — accountability

An authorised firm's governing body is accountable for:

(a) the development and oversight of the firm's business strategy and objectives;

(b) the firm's risk management framework;

(c) the firm's internal controls and assurance framework; and

(d) the firm's financial soundness.

3.1.10 General obligations — culture and values

An authorised firm's governing body must play the leading role in establishing the firm's corporate culture and values.

Guidance

To comply with this obligation, the governing body may need to develop and oversee a code of conduct or code of ethics for all employees that defines acceptable and unacceptable behaviour, and reminds them not to engage in illegal activity.

3.1.11 General obligations — own structure

An authorised firm's governing body:

(a) must have a well-designed governance structure;

Guidance

The governing body should maintain and periodically update rules, by-laws or other similar documents setting out its organisation, rights, responsibilities and key activities.

(b) must allocate sufficient time and attention for its members to perform their duties effectively; and

(c) must consider how it can best perform its role, and in particular whether to create 1 or more committees to make recommendations to the body on matters about which the body must make decisions.

3.1.12 General obligations — oversight

An authorised firm's governing body:

(a) must provide effective oversight of the individual who exercises the firm's senior executive function and the firm's senior management;

(b) must hold the individual who exercises the senior executive function and the firm's senior management accountable for their actions;

(c) must set out the possible consequences (including dismissal) if those actions are not aligned with the body's performance expectations;

(d) must deal prudently with any conflicts of interest that may arise by ensuring that no individual or group of individuals unduly influences the body's decision-making;

(e) must approve the organisational structure and corporate governance framework through which the firm is managed and controlled;

(f) must ensure that the firm has succession plans for its key functions;

(g) must establish direct and independent contact with the firm's audit and risk functions (if any);

(h) must ensure that the firm has effective policies, procedures and controls to deter, prevent, detect, report and remedy fraud, and must ensure that appropriate resources are allocated for that purpose; and

(i) must maintain transparency and disclosure.

3.1.13 General obligations — subsidiaries

If an authorised firm that is incorporated in the QFC has 1 or more subsidiaries, wherever incorporated, the firm's governing body must ensure that the firm seeks to promote good governance in those subsidiaries.

Note For detailed obligations in relation to subsidiaries, see rule 3.3.18.

3.1.14 Specific obligations — approving and updating plans

(1) An authorised firm's governing body:

(a) must approve strategic and business plans appropriate to the nature, scale and complexity of the firm's business; and

(b) must update the plans regularly to take account of changes in the business environment.

(2) The strategic and business plans may be combined in 1 document.

3.1.15 Specific obligations — appointment etc of individuals for certain functions

(1) A decision about the appointment, remuneration, disciplining or dismissal, or the assessment of the performance, of either of the following individuals:

(a) an individual who is approved to exercise the senior executive function for an authorised firm;

(b) an authorised firm's internal auditor;

may be made only by:

(c) the firm's governing body;

(d) any relevant committee of the governing body; or

(e) the chair of the governing body, after consulting the governing body.

(2) A decision about the appointment, remuneration, disciplining or dismissal, or the assessment of the performance, of any of the following individuals:

(a) an individual who is approved to exercise the risk management function for an authorised firm;

(b) an individual who is approved to exercise the compliance oversight function for an authorised firm;

(c) an authorised firm's approved actuary;

may be made only by:

(d) the firm's governing body or any relevant committee of the governing body; or

(e) the firm's senior management, after consulting the governing body or the relevant committee of the governing body.

3.1.16 Specific obligations — remuneration policy

(1) An authorised firm's governing body must establish and maintain, for itself and the whole firm, a remuneration policy appropriate to the nature, scale and complexity of the firm's business.

Note Appropriate records must be kept of the firm's remuneration policies and procedures — see GENE, rule 6.1.1.

(2) The policy must set out the firm's remuneration arrangements, including:

(a) the objectives and structure of any performance-based component;

(b) performance measures that are in line with the firm's risk management strategy;

(c) the forms and mix of remuneration; and

Examples

1 fixed and variable components

2 cash and equity-related benefits

3 termination payments.

(d) eligibility for, and the timing of, payments.

(3) The policy:

(a) must be aligned to the firm's culture, its risk appetite statement, its long-term strategic direction and viability, financial goals and overall safety and soundness; and

Note For the requirement for a risk appetite statement, see rule 7.1.2 (5) (a).

(b) must appropriately balance risk and reward.

(4) The forms and mix of remuneration (in particular, performance-based remuneration) must be consistent with sound risk management.

(5) The timing of payments must take into account the timeframes within which risks associated with individuals' performance are likely to materialise.

(6) The policy:

(a) must permit any performance-based component of an individual's remuneration (or such a component of the remuneration of a class of individuals) to be deferred or reduced (including reduced to zero) if necessary:

(i) to protect the firm's financial soundness; or

(ii) to respond to significant unexpected or unintended consequences of the firm's activities; and

(b) if the policy provides for part of an individual's remuneration to be based on performance, must provide for that part to be repayable to the firm by an individual who received it if the firm is later satisfied that:

(i) the individual failed to meet the relevant performance measures; or

(ii) by excessive risk-taking, he or she contributed significantly to a negative financial performance by the firm.

(7) The policy must prohibit an individual who has received deferred remuneration in the form of equity, or in any other form that is linked to the firm's equity, from hedging his or her economic exposures to the resultant equity price risk before the equity or other remuneration is fully vested.

(8) A remuneration package offered by the firm (including any performance-based component):

(a) must encourage behaviour that supports the firm's long-term financial soundness and risk management strategy;

(b) must align remuneration with prudent risk-taking; and

(c) must incorporate adjustments to reflect:

(i) the outcomes of the firm's activities;

(ii) the risks related to those activities, taking account of the cost of the associated capital; and

(iii) the time necessary for the outcomes of those activities to be reliably measured.

(9) The governing body must periodically review the remuneration policy.

Guidance

1 Guaranteed bonuses should generally not be offered because such bonuses are not consistent with sound risk management and performance-based rewards.

2 Remuneration payments should be linked to performance over time and should be designed in a way that does not reward failure.

3 Any deferral of payment to an individual must take into account the risks associated with his or her performance that may materialise during the period of deferment (for example, the risk of an increase in the cost of capital required to support the risks that he or she took; uncertainties in the timing and likelihood of future revenues and expenses).

4 The application of any deferral of payment may vary depending on:

- the level of seniority or responsibility of the individual to whom the payment is due
- the nature of risks to which the firm is exposed
- any other relevant matters.

5 Nothing in rule 3.1.16 prevents a firm from adopting the remuneration policy of a member of the firm's corporate group, provided that:

- the policy is approved by the firm's governing body
- the policy complies with rule 3.1.16.

3.1.17 Specific obligations — business resilience and continuity plan

(1) An authorised firm's governing body must establish a business resilience and continuity plan to ensure, so far as practicable, that the firm can continue to fulfil its obligations under the law applicable in the QFC in the event of an interruption.

(2) The body must keep the plan under review and must ensure that it is tested at intervals determined by the body.

(3) The interval between tests must be appropriate to the nature, scale and complexity of the firm's business but must not be longer than 18 months.

(4) The Regulatory Authority may direct the firm to test the plan at any time in a way that the Authority considers appropriate.

3.1.18 Specific obligations — avoiding or mitigating conflicts of interest

(1) An authorised firm's governing body must ensure that each part of the firm's corporate governance framework, and of its risk management framework, is designed:

(a) to avoid conflicts of interest (or to mitigate such conflicts if it is not possible to avoid them); and

(b) to deal effectively with any conflict of interest that arises.

(2) The frameworks must require that:

(a) any conflict of interest that arises must be reported:

(i) to the firm's senior management, or, if the firm is a branch, to the body that is responsible for the branch; and

(ii) if it is not addressed within a reasonable time by the senior management, to the firm's governing body; and

(b) every 6 months, the firm's senior management must give the governing body a written summary of all conflicts of interest addressed by the senior management during the period.

(3) In this rule and rule 3.1.19, a reference to a firm's governing body is a reference to the board, membership, committee or body (whatever it is called) that is responsible for the firm's corporate governance framework and risk management framework in relation to conflicts of interest and periodic review.

Guidance

A conflict of interest involving a member of the firm's governing body is to be dealt with under the governing body's own conflicts policy, governance manual or terms of reference.

3.1.19 Specific obligations — periodic review

(1) An authorised firm's governing body must ensure that the firm's corporate governance framework and risk management framework are reviewed at least once every 3 years by:

(a) the firm's internal auditor; or

(b) an independent and objective external reviewer.

Note For the meaning of ***governing body*** in this rule, see rule 3.1.18 (3).

(2) The person who carries out the review must report in writing to the body within 30 days after the review is completed.

(3) The firm must give a copy of the report to the Regulatory Authority within 30 days after the firm's governing body receives the report.

(4) The Authority may direct an authorised firm to carry out more frequent reviews than are required by subrule (1).

3.1.20 Specific obligations — keeping minutes

(1) The governing body of an authorised firm that is incorporated as a company in the QFC, and each committee of such a body, must maintain appropriate records of its deliberations and decisions, sufficient to show that the body or committee is effective and has carried out its responsibilities.

(2) The governing body of a branch must maintain appropriate records of its deliberations and decisions, sufficient to show that the governing body is effective and has carried out its responsibilities.

3.1.21 Specific obligations — independence of certain employees

(1) An authorised firm's governing body must ensure that each employee to whom a responsibility is allocated within the firm's internal controls framework is sufficiently free from influence for the framework to be effective in achieving its purposes.

(2) The requirement in subrule (1) is satisfied if reasonable measures have been taken to ensure that:

(a) no such employee is remunerated in a way that would tend to undermine his or her independence and objectivity in performing his or her duties;

Note For the requirements relating to a firm's remuneration policy, see rule 3.1.16.

(b) no such employee is involved in performing a function that generates, or is intended to generate, revenue for the firm;

(c) no such employee is limited or restricted as to the matters that he or she can investigate or report on in the exercise of his or her function;

(d) the reports and conclusions of such an employee can be honest and candid, without fear of reprisal; and

(e) pressure or influence is not applied to such an employee to modify his or her reports or conclusions.

Division 3.1.D Governing bodies — individual members' obligations

3.1.22 Obligations of individual members of governing body

A member of the governing body of an authorised firm:

(a) must act in good faith, honestly and reasonably;

(b) must exercise due care and diligence;

(c) must act in the best interests of the firm and its customers, putting those interests ahead of his or her own interests;

(d) must exercise independent judgment and objectivity in decision-making, taking due account of the interests of the firm and its customers; and

(e) must not use his or her position to gain undue personal advantage or cause detriment to the firm.

Part 3.2 Governing bodies — branches

3.2.1 Governing body composition and operations

(1) The governing body of an authorised firm that is a branch must have at least 3 members.

(2) The governing body must have a mix of relevant competencies, and as a whole must have the necessary skills to oversee the firm effectively.

Guidance

Relevant competencies include financial markets, financial analysis, financial stability issues, financial reporting, information technology, strategic planning, risk management, compensation, regulation, corporate governance and management skills.

(3) The governing body of an authorised firm that is a branch must meet at least every 3 months and at least 4 times in a year.

Part 3.3 Governing bodies — firms incorporated in QFC

3.3.1 Application of Part 3.3

This Part applies to an authorised firm that is incorporated in the QFC.

3.3.2 Meaning of *category A firm* and *category B firm*

In these rules:

category A firm means an authorised firm that is incorporated under the Companies Regulations and is:

(a) a banking business firm (within the meaning given by BANK, rule 1.3.1);

(b) an Islamic banking business firm (within the meaning given by IBANK, rule 1.1.9);

(c) a QFC insurer (other than a QFC captive insurer); or

(d) a takaful entity (within the meaning given by PINS, rule 1.2.7).

category B firm means an authorised firm that is incorporated in the QFC but is not a category A firm.

3.3.3 References in Part 3.3 to *board of directors* etc

(1) In these rules, the members of the governing body of an authorised firm, and the governing body itself, are generally referred to as such. In this Part, the governing body of an authorised firm is referred to as its ***board of directors*** or just ***board*** and the members of the board are referred to as ***directors***.

(2) In these rules, a reference to a ***director*** of an authorised firm includes any person in accordance with whose instructions the firm customarily acts.

3.3.4 Meaning of *non-executive director* and *Independent non-executive director*

In these rules:

independent non-executive director of an authorised firm means a non-executive director who is eligible, under rule 3.1.3, as an independent non-executive member of the firm's board.

non-executive director of an authorised firm means a director who has no responsibility for implementing the decisions or the policies of the firm's board.

3.3.5 Firms listed on Qatar Exchange

An authorised firm that is listed on the Qatar Exchange must comply with both this Part and the governance rules of that Exchange. In any case in which this Part and those rules impose different obligations, the firm must comply with whichever obligation is the more onerous.

3.3.6 Number of directors

(1) An authorised firm must ensure that its board of directors is of sufficient size and expertise to adequately oversee the operation of the firm.

(2) The board of a category A firm must be made up of:

(a) at least 5 directors; or

(b) a greater number directed by the Regulatory Authority.

(3) The board of a category B firm must be made up of:

(a) at least 3 directors; or

(b) a greater number directed by the Authority.

(4) In a direction under paragraph (2) (b) or (3) (b), the Authority may specify how many executive directors or independent non-executive directors (or both) that the relevant firm's board must have.

(5) A majority of the members of the board of a category A firm must be non-executive directors, and a majority of the non-executive directors must be independent non-executive directors.

(6) A majority of the members of the board of a category B firm must be non-executive members, and at least 1 of the non-executive members must be an independent non-executive member.

(7) In the case of a category A firm that is a subsidiary, the majority of its board's members may be directors or senior executives of the parent firm or another member of the corporate group. However, the authorised firm must still have at least 2 independent non-executive directors.

3.3.7 Board competencies

The directors of an authorised firm must have a mix of relevant competencies, and as a whole must have the necessary skills to oversee the firm effectively.

Guidance

Relevant competencies include financial markets, financial analysis, financial stability issues, financial reporting, information technology, strategic planning, risk management, compensation, regulation, corporate governance and management skills.

3.3.8 Category A firms—board committees to be established

(1) The board of directors of a category A firm must establish the following committees:

(a) nominations committee;

(b) remuneration committee;

(c) audit committee;

(d) risk committee.

(2) The chair of each committee must be an independent non-executive director.

(3) With the written consent of the Regulatory Authority, a category A firm:

(a) may combine the nomination committee and the remuneration committee; and

(b) may combine the audit committee and the risk committee.

(4) Each committee must have clear terms of reference setting out its role and objectives and the authority delegated to it by the board.

(5) Each committee:

(a) must report regularly to the board; and

(b) must circulate its minutes to all of the members of the board.

3.3.9 Category B firms—board committees

(1) The board of a category B firm may establish some, or all, or none of the committees mentioned in rule 3.3.8 (1).

(2) If the board of a category B firm does not establish any 1 or more of those committees, the full board must discharge the responsibilities of any committee that is not established.

Note Those responsibilities are described in rules 3.3.10, 3.3.11 (1), 3.3.12 (1) and 3.3.13 (1).

3.3.10 Nominations committee

The nominations committee is responsible for making recommendations to the board for the appointment of new board members, individuals to be appointed to exercise the senior executive function, and senior management.

3.3.11 Remuneration committee

(1) The remuneration committee is responsible for developing, adopting and overseeing a written remuneration policy for the firm, and in particular for the remuneration of the board and senior management.

Note For the requirements about the remuneration policy, see rule 3.1.16.

(2) All of the members of the remuneration committee must be non-executive directors.

3.3.12 Audit committee

(1) The audit committee is responsible for:

(a) adopting and overseeing a written policy on internal audit and financial reporting;

(b) reviewing the results of the audit process with management and external auditors;

(c) overseeing the firm's internal auditors and interacting with the external auditors;

(d) making decisions (or recommendations to the board or shareholders) about the appointment, remuneration and dismissal of external auditors;

(e) reviewing and approving the scope and frequency of audit;

(f) receiving significant audit reports and ensuring that senior management promptly takes any corrective action that is necessary to address control weaknesses, non-compliance with policies, laws and regulations, and other problems;

(g) overseeing the establishment of accounting policies and practices;

(h) reviewing third-party opinions on the design and effectiveness of the overall internal controls and assurance framework; and

(i) if the firm is an Islamic financial institution:

(i) reviewing the effectiveness of its systems and controls for monitoring compliance with Shari'a (including reviewing the reports of internal Shari'a reviews and the Shari'a supervisory board to ensure that appropriate action has been taken); and

(ii) ensuring that the firm's reporting of financial information complies with internationally recognised accounting standards that comply with Shari'a.

(2) A majority of the members of the audit committee must be non-executive directors.

(3) The chair of the board must not be a member of the audit committee.

(4) The audit committee must meet at least 4 times a year.

3.3.13 Risk committee

(1) The risk committee is responsible for:

(a) advising the board on the firm's overall risk appetite, overseeing senior management's implementation of the firm's risk management strategy, reporting on the firm's risk culture, and interacting with and overseeing the firm's risk management function;

Note For the requirements relating to the risk management strategy, see rule 7.1.4.

(b) overseeing the firm's strategies for:

(i) the management of the firm's capital and liquidity; and

(ii) dealing with all the relevant risks;

to ensure that the strategies are consistent with the firm's risk appetite; and

(c) receiving regular reports about:

(i) the firm's risk profile;

(ii) measurement against the approved risk appetite and risk limits; and

(iii) any limit breaches and actions taken as a result of such breaches.

(2) A majority of the members of the risk committee must be non-executive directors.

3.3.14 Frequency of board meetings

(1) The board of directors of a category A or category B firm must meet:

(a) at least every 3 months and at least 4 times in a year; or

(b) more frequently, if the Regulatory Authority so directs.

(2) In a direction under paragraph (1) (b), the Authority may specify how often the board must meet, or how long may pass between meetings, or both, taking into account the nature, scale and complexity of the firm's operations.

3.3.15 Chair of the board

(1) The chair of the board of a category A or category B firm must be a non-executive director.

Guidance

The Regulatory Authority expects that the chair of a category A firm that is not a subsidiary will be an independent non-executive director.

(2) If the chair of a category A firm that is not a subsidiary is not an independent non-executive director, the firm must be able to demonstrate how its governance arrangements will satisfy the need for independent oversight of the firm's senior management.

Guidance

The independent oversight referred to in subrule (2) could be provided by, for example, nominating a senior independent non-executive director with explicit responsibilities in this regard.

(3) The chair of the board of a category A or category B firm must not have been an employee of the firm during the previous 5 years.

(4) The chair is responsible for the following:

(a) setting the board's agenda and ensuring that every agenda item (particularly any item dealing with strategic and risk issues) receives sufficient attention;

(b) ensuring that every board member receives thorough, relevant and accurate background information in time for each meeting;

(c) encouraging transparent and candid debate by promoting contributions by all the members, particularly the non-executive directors and independent non-executive directors.

3.3.16 Training and competency of board members

(1) A member of the board of a category A or category B firm must regularly update and refresh his or her skills and knowledge.

(2) The board of a category A or category B firm must ensure that:

(a) a suitable induction program is offered to a newly-appointed board member to help him or her to understand the duties and role of a member; and

(b) regular updates and training are offered to each board member to maintain the member's competency for that role.

3.3.17 Periodic assessments of performance

(1) The board of a category A or category B firm must regularly assess (with the assistance of external experts, if necessary) the performance of the board as a whole, of its committees and of each board member. The assessments:

(a) must review the board's structure, size and composition and the structures and coordination of the committees;

(b) must consider:

(i) rotating the members and chairs of committees periodically; and

(ii) limits to tenure on the board or on a committee;

(c) must assess each committee's performance against its terms of reference; and

(d) must assess each board member's suitability, taking into account the member's performance on the board.

(2) A category A firm must carry out the assessments required by subrule (1) annually. A category B firm must carry out those assessments at least once every 3 years.

(3) The board must review the effectiveness of its own governance practices and procedures, must determine where improvements may be needed, and must make any necessary changes. The board may do so either separately or as part of an assessment required by subrule (1).

(4) The board must use the results of the assessments required by subrules (1) to (3) as part of its efforts toward continuing to improve the board.

3.3.18 What if authorised firm is parent company of corporate group?

(1) If a category A or category B firm is the parent company of a corporate group, the firm's board must ensure that it is aware of the material risks and issues that affect both the firm and its subsidiaries. The board must exercise adequate oversight over the subsidiaries while respecting the subsidiaries' legal and governance responsibilities.

(2) In particular, the board must ensure that it understands the purpose, structure, governance and unique risks of the firm's subsidiaries.

(3) The board:

(a) must establish a group structure (including the legal entity and business structure) and a corporate governance framework with clearly defined roles and responsibilities, at the parent company level and at the subsidiary level, as appropriate, based on the complexity and significance of each subsidiary;

(b) must define an appropriate subsidiary board and management structure that takes into account the material risks to which the group, its businesses and its subsidiaries are exposed;

(c) must assess whether the group's corporate governance framework:

(i) includes adequate policies, processes and controls; and

(ii) addresses risk management across the businesses and legal entity structures;

(d) must ensure that the group's corporate governance framework includes appropriate processes and controls to identify and address potential intragroup conflicts of interest (such as those arising from intragroup transactions);

(e) must approve policies and clear strategies for establishing new structures and legal entities, and must ensure that the policies and strategies are consistent with the policies and interests of the group;

(f) must assess whether there are effective systems to exchange information among the various entities, to manage the risks of the subsidiaries and of the group as a whole, and to ensure that the group is effectively supervised;

(g) must allocate sufficient resources to monitor the compliance of the subsidiaries with all applicable legal, regulatory and governance requirements;

(h) must maintain an effective relationship with the Regulatory Authority and, through the subsidiaries' boards or direct contact, with the regulators of all the subsidiaries; and

(i) must establish an effective internal audit function that ensures that audits are performed within or for all the subsidiaries and parts of the group and the group as a whole.

Part 3.4 Statements of compliance with Chapter 3

3.4.1 Annual compliance statement

(1) An authorised firm must give a written statement to the Regulatory Authority every year as to the extent to which it has complied with the applicable requirements of this Chapter during the previous year.

(2) If the firm has not fully complied with an applicable requirement of this Chapter, the statement must set out:

(a) the requirement with which the firm has not complied;

(b) the reasons for the non-compliance; and

(c) a statement of what the firm is doing or intends to do to bring itself into compliance with the requirement.

(3) The statement must be signed by:

(a) either:

(i) if the firm is incorporated in the QFC — the chair of the firm's board of directors; or

(ii) for any other authorised firm — the chair of the firm's governing body; and

(b) the individual who is approved to exercise the senior executive function for the firm.

(4) If the firm is incorporated in the QFC, the firm:

(a) must provide the statement to its shareholders no later than the date on which it must provide them with its annual report; and

(b) must make the statement available on its website.

Chapter 4 Senior management

Notes for Chapter 4

1 The senior management of an authorised firm is made up of the individuals who are approved to exercise the controlled functions mentioned in rule 4.1.1 (a). Although the individuals who are approved to exercise the MLRO function and the internal control and assurance functions (risk management function, compliance oversight function, internal audit function and actuarial function) form part of an authorised firm's senior management, those controlled functions are not specifically further dealt with in Chapter 4.

2 For firms' obligations in relation to the MLRO function, see:

- for general insurance firms — AMLG
- for all other authorised firms — AML/CFTR.

3 The internal control and assurance functions are dealt with in Chapter 6.

4.1.1 What is an authorised firm's *senior management*?

An authorised firm's ***senior management*** is made up of:

(a) each individual (if any) who is approved to exercise any of the following controlled functions for the firm:

(i) the senior executive function;

(ii) the finance function;

(iii) the senior management function;

(iv) the MLRO function;

(v) the risk management function;

(vi) the compliance oversight function;

(vii) the internal audit function;

(viii) the actuarial function; and

(b) any other individual who, in the Regulatory Authority's opinion, has overall responsibility for the day-to-day management of the part or parts of the firm's business in or from the QFC.

Guidance

1 FSR article 31 provides that, subject to that article, the Regulatory Authority may:

(a) impose or vary such conditions, restrictions and requirements on an authorisation as the Authority considers appropriate; or

(b) require a person specified in the condition, restriction or requirement to take or refrain from taking such action as the Authority considers appropriate.

2 For this Part, the powers in FSR article 31 enable the Authority, for example, to direct a firm:

- to appoint, to exercise a controlled function, an individual who is ordinarily resident in Qatar even if this Part does not require the individual to be so resident
- to appoint an individual to exercise a controlled function even if this Part does not require the firm to have such an individual.

4.1.2 Senior management's role

The members of an authorised firm's senior management are collectively responsible for implementing the corporate governance framework and risk management framework approved by the firm's governing body, and for overseeing the firm's daily operations. The members of the senior management:

(a) must ensure that the implementation of the frameworks is in accordance with these rules;

(b) must discharge their management responsibilities conscientiously and prudently;

(c) must maintain clear decision-making procedures to the extent appropriate to the nature, scale and complexity of the firm's business;

(d) must actively promote a strong governance and risk management culture throughout the firm; and

(e) must establish and maintain policies and procedures that enable them to be satisfied that any individual who is to act for the firm is suitable, having regard to:

(i) the role that he or she is to have in the firm; and

(ii) the law applicable in the QFC.

4.1.3 Duties of individuals towards firm

Each member of an authorised firm's senior management owes the following duties to the firm:

(a) to act for the firm's benefit;

(b) to avoid any conflict between his or her interests and those of the firm (or, if it is not possible to avoid such a conflict, to mitigate it);

(c) to have, and to maintain, the knowledge and skills that are reasonably expected of an individual who holds a similar appointment, and carries out similar functions, in the senior management of the firm;

(d) to carry out his or her functions diligently.

4.1.4 Requirement for firms to have senior executive function

(1) An authorised firm must have an individual who is approved to exercise the senior executive function for the firm.

(2) The individual must be ordinarily resident in Qatar.

4.1.5 Requirement for firms to have finance function

An authorised firm must have an individual who is approved to exercise the finance function for the firm.

Chapter 5 Controlled functions generally

5.1.1 Exercise of 2 or more controlled functions by same individual

(1) Subject to subrule (2), an individual may exercise 2 or more controlled functions for an authorised firm if (but only if):

(a) the firm's governing body confirms to the Regulatory Authority in writing that it is satisfied that:

(i) the individual's exercise of those controlled functions in combination:

(A) does not give rise to any internal or external conflict of interest; and

(B) does not compromise the independence, objectivity and effectiveness of the exercise of any of the functions;

(ii) the individual's combined exercise of the functions will not increase the firm's risk of non-compliance with the law applicable in the QFC or any other applicable law; and

(iii) it is not inappropriate, having regard to the nature, scale and complexity of the firm's business, for the individual to exercise both or all of the controlled functions; and

(b) the Authority is satisfied that:

(i) the conditions in subparagraphs (a) (i), (ii) and (iii) have been met; and

(ii) the individual can adequately exercise the functions in combination.

(2) An authorised firm must not combine the internal audit function with any other controlled function.

(3) At least once in every year, the firm's senior management must review:

(a) the firm's policies, procedures and controls for combining the functions, including its procedures for assessing:

(i) whether it is feasible to continue to combine the functions;

(ii) the risk in doing so; and

(iii) the likely effect of doing so on the firm's business; and

(b) the combined exercise of the functions, to satisfy itself that:

(i) the combined exercise does not compromise the independence, objectivity and effectiveness of the exercise of each function;

(ii) no internal or external conflict of interest arises;

(iii) the combined exercise has not increased, and will not increase, the firm's risk of non-compliance with the law applicable in the QFC or any other applicable law; and

(iv) the combined exercise continues to be appropriate, having regard to the nature, scale and complexity of the firm's business.

(4) The senior management must report the results of a review under subrule (2) to the firm's governing body within 30 days after the review is completed.

(5) If the Regulatory Authority is satisfied that it is no longer appropriate for 2 or more controlled functions to be exercised for an authorised firm by the same individual, the Authority may, by written notice, direct the firm to do either or both of the following:

(a) stop combining the functions;

(b) appoint 1 or more individuals to exercise any of the functions.

(6) In particular, the Authority may give a direction under subrule (4) if the Authority considers that:

(a) the continued performance by the individual of both or all the functions:

(i) is no longer appropriate, having regard to the nature, scale and complexity of the firm's business;

(ii) has given rise, or is likely to give rise, to an internal or external conflict of interest; or

(iii) has compromised, or is likely to compromise, the independence, objectivity and effectiveness of the performance of any of the functions;

(b) the individual is performing any of the functions at a standard that is below the standard at which a reasonable person having the necessary skills, knowledge and experience would be expected to perform that function; or

(c) the combined performance of the functions by the individual has impaired, or is likely to impair, the firm's compliance with the requirements applicable to the conduct of its business in or from the QFC.

5.1.2 Performing controlled functions within a corporate group

An individual may exercise a controlled function for more than 1 authorised firm if the firms are part of the same corporate group or are owned by the same shareholders.

Chapter 6 Internal controls and assurance

Note for Chapter 6

An authorised firm's ***internal control and assurance framework*** is made up of the policies, processes, tasks, behaviours and other aspects of its organisation that, taken together:

- enable the firm to respond appropriately to business, operational, financial, compliance and other risks, and so facilitate its effective operation
- safeguard the firm's assets and ensure that its liabilities are identified and managed
- ensure the quality of the firm's internal and external reporting (which requires proper records and processes that generate a flow of timely, relevant and reliable information from internal and external sources)
- ensure that the firm complies with applicable laws and regulations and with its internal policies.

Part 6.1 General

6.1.1 Objectives of internal controls and assurance framework

An authorised firm must establish and maintain an internal controls and assurance framework to ensure that:

(a) the firm's business is conducted efficiently;

(b) the firm's assets are safeguarded;

(c) fraud and other unlawful acts are prevented or detected;

(d) risk is managed effectively;

(e) the firm's financial records are accurate and complete; and

(f) the preparation of the firm's financial statements is timely.

6.1.2 Independence of internal control and assurance functions etc

(1) An authorised firm must ensure that each individual who exercises an internal control and assurance function is sufficiently free from influence to be effective in achieving the function's purpose.

(2) The requirement in subrule (1) is satisfied if reasonable measures have been taken to ensure that:

(a) no such individual is remunerated in a way that would tend to undermine his or her independence and objectivity in exercising the function;

Note For the requirements relating to a firm's remuneration policy, see rule 3.1.16.

(b) no such individual is involved in performing a function that generates, or is intended to generate, revenue for the firm;

(c) no such individual is limited or restricted as to the matters that he or she can investigate or report on in the exercise of his or her function;

(d) the reports and conclusions of such an individual can be honest and candid, without fear of reprisal; and

(e) pressure or influence is not applied to such an individual to modify his or her reports or conclusions.

Guidance

An internal control and assurance function cannot be effective unless its exercise is independent. ***Independent*** means, broadly, that the individual who exercises the function is not subjected to pressure to mould or manipulate his or her conclusions or results. An internal control and assurance function that produces only results that are convenient to the firm's governing body or management would not be regarded as satisfying rule 6.1.1.

(3) An authorised firm must ensure that:

(a) each individual who exercises an internal control and assurance function; and

(b) each employee who is allocated responsibilities within the firm's corporate governance framework and its risk management framework;

has all of the following:

(c) the necessary authority to exercise the function or carry out his or her duties;

(d) access to all necessary information, documents and records of the firm;

(e) appropriate access to the firm's governing body and senior management.

6.1.3 Direct access to governing body by certain individuals

An authorised firm's policies, procedures and controls must provide that an individual who is approved to exercise an internal control and assurance function for the firm is entitled to raise matters directly with the firm's governing body, the chair of the body, or any relevant committee of the body, and to do so privately (that is, without the presence of any representative of the firm's senior management).

6.1.4 Certain individuals' obligation to raise matters promptly

An authorised firm's policies, procedures and controls must provide that an individual who is approved to exercise an internal control and assurance function for the firm:

(a) must promptly raise significant matters directly with the firm's governing body, the chair of the body, or any relevant committee of the body; and

(b) must promptly tell any other individual to whom this rule applies if the first individual becomes aware of a risk that might have (or a number of risks that, taken together, might have) a significant effect on:

(i) the firm's risk management strategy; or

(ii) the other individual's functions.

6.1.5 Reports about internal control and assurance functions

(1) An authorised firm must ensure that each internal control and assurance function makes periodic written reports to the firm's governing body, or a relevant committee of the body, about the matters in subrule (2).

(2) The matters are the following:

(a) how each internal control and assurance function is performing against the firm's policies, procedures and controls for the function;

(b) the shorter-term and longer-term objectives of each internal control and assurance function, and the progress made in achieving those objectives;

(c) resources of staff, equipment, time and budget allocated to the internal controls and assurance framework and an analysis of the adequacy of those resources;

(d) any material deficiency, material weakness or material failure of an internal control and assurance function, and the response to the deficiency, weakness or failure.

Guidance

The body or committee could also have regard to:

- reports by the internal audit function that cover the other internal control and assurance functions
- reports commissioned from third parties in relation the internal control and assurance functions.

(3) The body or committee must determine:

(a) how often such a report must be made; and

(b) how serious a deficiency, weakness or failure must be to require reporting under subrule (2) (d).

Note Under GENE, rule 4.1.3 (2) (g), an authorised firm must immediately tell the Regulatory Authority about any material deficiency, material weakness or material failure in the firm's internal control and assurance functions.

Part 6.2 Risk management function

6.2.1 Authorised firms to have risk management function

An authorised firm must establish and maintain a risk management function that is appropriate to the nature, scale and complexity of the firm's business.

6.2.2 What makes up authorised firm's *risk management function*?

(1) An authorised firm's ***risk management function*** is made up of:

(a) the individual (if any) who is approved to exercise the risk management function for the firm;

(b) any other employees allocated to the function;

(c) the part of the firm's resources (other than staff) allocated to the function;

(d) the firm's risk management strategy;

(e) the firm's risk management policy; and

(f) the records that the firm keeps in relation to risk management.

Note 1 For the requirements relating to the risk management strategy, see rule 7.1.4.

Note 2 There are also specific requirements in PINS for a QFC insurer's risk management strategy and policy. See PINS, Chapter 2.

(2) The purpose of an authorised firm's risk management function is to monitor and control the firm's risk exposure.

(3) The risk management function must provide for timely monitoring of, advising on, investigating and reporting on all reasonably foreseeable material risks.

6.2.3 Which firms must have individual to exercise risk management function?

(1) A QFC bank must have an individual who is approved to exercise the risk management function for the firm.

(2) A QFC insurer (other than a QFC captive insurer) must have an individual who is approved to exercise the risk management function for the firm.

Note ***QFC bank***, ***QFC insurer*** and ***QFC captive insurer*** are defined in the Glossary.

(3) Any other authorised firm must have an individual who is approved to exercise the risk management function for the firm if it is appropriate to do so because of the nature, scale and complexity of the firm's business.

(4) The individual who is approved to exercise the risk management function for the following firms must be ordinarily resident in Qatar:

(a) a QFC bank;

(b) a QFC insurer (other than a QFC captive insurer) that is incorporated under the Companies Regulations.

Part 6.3 Compliance oversight function

6.3.1 Which firms must have compliance oversight function?

An authorised firm must establish and maintain a compliance oversight function that is appropriate to the nature, scale and complexity of the firm's business.

6.3.2 Which firms must have individual to exercise compliance oversight function?

(1) An authorised firm must have an individual who is approved to exercise the compliance oversight function for the firm.

(2) The individual who is approved to exercise the compliance oversight function for the following firms must be ordinarily resident in Qatar:

(a) a QFC bank;

(b) a QFC insurer (other than a QFC captive insurer) that is incorporated under the Companies Regulations.

6.3.3 What makes up authorised firm's *compliance oversight function*?

(1) An authorised firm's ***compliance oversight function*** is made up of:

(a) the individual who is approved to exercise the compliance oversight function for the firm;

(b) any other employees allocated responsibilities within the function;

(c) the part of the firm's resources (other than staff) allocated to the function;

(d) the firm's compliance policies and procedures; and

(e) the records that the firm keeps in relation to compliance matters.

Note Appropriate records must be kept of policies and procedures — see GENE, rule 6.1.1.

(2) The purposes of an authorised firm's compliance oversight function are the following:

(a) to ensure that the firm complies with:

(i) decisions of the Regulatory Authority;

(ii) the firm's internal policies, procedures and controls; and

(iii) requirements and standards applicable to the firm under the law applicable in the QFC or any other applicable law;

(b) to ensure that the firm's business is conducted ethically and responsibly;

(c) to minimise the risk of the firm or its facilities being used in the furtherance of financial crime.

Guidance

The compliance oversight function includes:

- monitoring and assessing the adequacy and effectiveness of the firm's compliance policies and procedures
- participating in the process of approving new products or significant changes to existing products
- monitoring and assessing the extent to which it complies with those policies and procedures
- monitoring and assessing the adequacy and effectiveness of measures taken to correct any deficiencies
- reporting to the firm's governing body as necessary
- maintaining and updating the firm's compliance policies and procedures in conjunction with the firm's senior executive function and senior management
- providing advice and support to the firm's senior executive function and senior management about compliance issues.

Note For the meaning of ***financial crime***, see the Glossary.

Part 6.4 Internal audit function

6.4.1 Which firms must have internal audit function?

(1) A QFC bank or a QFC insurer (other than a QFC captive insurer) must establish and maintain an internal audit function.

(2) An authorised firm that is not required by subrule (1) to have an internal audit function must establish and maintain such a function if it is appropriate to do so because of the nature, scale and complexity of the firm's business.

(3) The Regulatory Authority may direct an authorised firm to establish and maintain an internal audit function.

(4) An authorised firm's internal audit function must be appropriate to:

(a) the nature, scale and complexity of the firm's business; and

(b) the firm's risk profile and legal status.

6.4.2 Which firms must have internal auditor?

(1) A QFC bank must have an individual who is approved to exercise the internal audit function for the firm.

(2) A QFC insurer (other than a QFC captive insurer):

(a) must have an individual who is approved to exercise the internal audit function for the firm; or

(b) may, with the permission of the Regulatory Authority, appoint a suitably qualified third party as internal auditor.

(3) For Part 8.2, the appointment of a third party by a QFC insurer is a material outsourcing arrangement.

(4) Any other authorised firm must have an individual who is approved to exercise the internal audit function for the firm if it is appropriate to do so because of the nature, scale and complexity of the firm's business.

(5) The Authority may direct an authorised firm to appoint an individual who is approved to exercise the internal audit function for the firm.

Guidance

For a firm that is part of a corporate group, the corporate group internal audit function may be used to perform the function for the firm. This means that the firm is not required to have a dedicated resource for the internal audit function. The work to be undertaken by the internal audit function would depend on the agreed risk-based audit plan for the firm and the corporate group-wide auditor would be best placed to decide that work.

Note Nothing in this rule prevents a firm from appointing a corporate group employee to the internal audit function.

6.4.3 What makes up authorised firm's *internal audit function*?

(1) An authorised firm's ***internal audit function*** is made up of:

(a) the firm's internal auditor (if any);

(b) any other employees who are allocated responsibilities within the function;

(c) the part of the firm's resources (other than staff) allocated to the function;

(d) the firm's audit charter and risk-based audit plan; and

(e) the records that the firm keeps in relation to internal audit.

Note For other audit requirements for firms, see GENE, Part 9.5.

(2) The purpose of an authorised firm's internal audit function is to provide independent assurance of:

(a) the adequacy and effectiveness of the firm's policies and procedures, and the documentation about them, for the firm as a whole, its corporate group, each subsidiary (if any) and each part of the firm (such as a business unit, business area or department);

(b) the reliability and integrity of information and the means used to identify, measure, classify and report such information;

(c) the accuracy and currency of the identification of risks and the agreed actions to address them;

(d) the safeguarding of the firm's assets and the assets of its depositors, policyholders, clients and other stakeholders;

(e) the existence of those assets;

(f) whether the firm's assets are appropriately segregated from the assets of its depositors, policyholders, clients and other stakeholders; and

(g) the performance of the firm's external auditors, to the extent requested by its governing body and consistent with applicable law.

(3) The internal audit function must carry out regular assessments of the firm's internal audit policies, procedures and controls and incorporate any necessary improvements.

6.4.4 Authority of internal auditor

An authorised firm's internal audit policies, procedures and controls must provide that:

(a) the firm's internal auditor, and any employee allocated responsibilities within the internal audit function, must have access to, and must review, any information, documents and records of the firm that he or she considers necessary to carry out an audit or other review; and

(b) the internal auditor has the authority:

(i) to undertake, on his or her own initiative, a review of any area or any function of the firm consistently with the internal audit function's purpose;

(ii) to require an appropriate management response to an internal audit report, including the development of a suitable remediation or mitigation plan or other follow-up plan; and

(iii) to decline to undertake an audit or review, or take on any other duty, that he or she believes is inconsistent with the internal audit function's purpose or the firm's internal audit policies and procedures.

Part 6.5 Actuarial function

6.5.1 Which QFC insurers must have actuarial function?

(1) This rule applies to a QFC insurer if:

(a) the insurer conducts long term insurance business (within the meaning given by PINS, rule 1.2.5 (2)); or

(b) the insurer conducts general insurance business (within the meaning given by PINS, rule 1.2.5 (1)), and:

(i) more than 15% of the insurer's gross outstanding liabilities are attributable to contracts of insurance for general insurance business in PINS category 1; or

(ii) more than 20% of the insurer's gross outstanding liabilities are attributable to contracts of insurance for general insurance business in PINS category 4.

(2) However, this rule does not apply to a QFC captive insurer.

Note For the obligations of a QFC captive insurer in relation to the actuarial function, see CAPI, Chapter 7.

(3) A QFC insurer to which this rule applies must establish and maintain an actuarial function that is appropriate to the nature, scale and complexity of the insurer's business.

(4) In subrule (1):

PINS category 1 and ***PINS category 4*** have the respective meanings given by PINS, rule 1.2.8.

6.5.2 Which QFC insurers must have individual to exercise actuarial function?

(1) A QFC insurer to which rule 6.5.1 applies must have an individual who is approved to exercise the actuarial function for the firm (an ***approved actuary***).

(2) The individual must not be one who:

(a) exercises the senior executive, executive governance or non-executive governance function for the insurer or a related body

corporate (except a related body corporate that is a subsidiary of the insurer); or

(b) is an employee or director of an approved auditor (under the Companies Regulations, article 85 (1)) for the insurer.

6.5.3 What makes up QFC insurer's *actuarial function*?

(1) A QFC insurer's ***actuarial function*** is made up of:

(a) each approved actuary for the insurer;

(b) any other employees who are allocated responsibilities within the actuarial function;

(c) the part of the insurer's resources (other than staff) allocated to the function;

(d) the insurer's actuarial policies and procedures; and

(e) the records that the insurer keeps in relation to actuarial matters.

Note See PINS, Chapter 9, for an insurer's obligations in relation to actuarial reporting.

(2) The purpose of the actuarial function of a QFC insurer is to advise the insurer on, and to monitor, investigate and report on, risks that materially affect:

(a) the insurer's ability to meet its liabilities to policyholders;

(b) its capital requirements and solvency position;

(c) its technical provisions; and

(d) the setting of its premiums or prices.

Guidance

The matters about which an insurer's actuary might advise the insurer include:

- the insurer's actuarial and financial risks
- its investment policies and the valuation of its assets
- its solvency position, including the calculation of the minimum capital required for regulatory purposes and liability and loss provision
- its prospective solvency position

- its risk management strategy, and its risk assessment and management policies, procedures and controls relevant to actuarial matters or the financial condition of the firm
- distribution of policy dividends or other benefits
- underwriting policies
- reinsurance arrangements
- product development and design, including the terms and conditions of insurance contracts
- the sufficiency and quality of data used to calculate technical provisions
- risk modelling in the insurer's own risk and solvency assessment
- the insurer's use of internal models.

6.5.4 QFC insurer to give notice before removing approved actuary

(1) A QFC insurer that has an approved actuary must give the Regulatory Authority reasonable advance notice of any intention to remove the actuary.

(2) The notice must set out the reasons for the removal.

6.5.5 QFC insurer to give notice if appointment of approved actuary ends

If the appointment of a QFC insurer's approved actuary ends for any reason, the insurer must tell the Regulatory Authority immediately, but by no later than the second business day after the day the appointment ends:

(a) that the appointment has ended; and

(b) the reasons for the ending of the appointment.

Note For the obligation of the approved actuary to notify the Regulatory Authority if his or her appointment ends, see FSR, article 91 (Resignation of auditors and actuaries).

6.5.6 QFC insurer to appoint actuary if vacancy arises

If at any time there is no approved actuary for a QFC insurer to which rule 6.5.1 applies, the insurer must appoint an individual to the

actuarial function as soon as practicable, but within 3 months after the day the vacancy arises.

6.5.7 Authority of QFC insurer's approved actuary

The actuarial policies, procedures and controls of a QFC insurer to which rule 6.5.1 applies must provide that:

(a) the insurer's approved actuary must have access to, and must review, any information, documents and records of the insurer that he or she considers necessary to carry out a review; and

(b) the approved actuary has the authority:

(i) to undertake, on his or her own initiative, a review of any area or any function of the insurer consistently with the actuarial function's purpose;

(ii) to require an appropriate management response to an actuarial report, including the development of a suitable remediation or mitigation plan or other follow-up plan; and

(iii) to decline to undertake a review, or take on any other duty, that he or she believes is inconsistent with the actuarial function's purpose or the insurer's actuarial policies and procedures.

6.5.8 Regulatory Authority may appoint actuary in certain circumstances

(1) If no individual is approved to exercise the actuarial function for a QFC insurer to which rule 6.5.1 applies within 28 days after a vacancy arises, the Regulatory Authority may appoint an actuary, or 2 or more actuaries, to exercise any part of the actuarial function for the insurer on the following terms:

(a) the insurer is to remunerate the actuary or actuaries on a basis agreed between the insurer and the actuary or, if there is no agreement, on a reasonable basis;

(b) each actuary is to hold office until he or she resigns or an actuary is approved for the insurer;

(c) each actuary has the same authority within the insurer that he or she would have as an approved actuary.

(2) The insurer must comply with, and is bound by, the terms on which the Authority appoints an actuary under subrule (1).

(3) An actuary appointed by the Authority under subrule (1) is not an approved actuary.

Guidance

1 Rule 6.5.8 allows, but does not require, the Regulatory Authority to appoint an actuary if no actuary has been approved for the insurer within the 28-day period referred to in rule 6.5.8 (1). In considering whether to use that power, the Authority would take into account the likely delay until the insurer can make an appointment, and the urgency of any pending duties of the actuary.

2 The Authority would not normally seek to appoint an actuary under rule 6.5.8 if the insurer concerned has applied for the approval of an individual to exercise the actuarial function and that application is still being considered.

3 If the Authority appoints an actuary, the insurer remains obliged to appoint an individual to the actuarial function and must seek the Authority's approval of the individual (even if the individual it proposes to appoint is the actuary appointed by the Authority).

Chapter 7 Risk management

7.1.1 Application of Chapter 7

This Chapter applies to all authorised firms.

Guidance

In assessing the appropriateness of an authorised firm's risk management framework, and the firm's compliance with the provisions of this Chapter, the Regulatory Authority will have regard to the firm's risk profile, and in particular to:

- the nature scale and complexity of operations in the QFC
- whether or not the firm is a branch of a firm established in another jurisdiction
- whether or not the firm is included in a risk management framework established at head office or group level.

7.1.2 Firms to have risk management framework

(1) An authorised firm must have a documented risk management framework.

(2) An authorised firm's risk management framework must enable the firm to appropriately develop and implement strategies, policies, procedures and controls to manage different types of material risks, and must provide the firm's governing body with a comprehensive firm-wide view of material risks.

(3) The framework must be appropriate to the nature, scale and complexity of the firm's business.

(4) An authorised firm that is a branch may rely on the risk management framework of its head office if the firm has assessed the head office's risk management framework and decided that it appropriately addresses the firm's internal and external sources of material risk.

(5) An authorised firm's risk management framework must reflect the firm's business objectives and the business plan approved by the firm's governing body, and must include all of the following:

(a) a risk appetite statement;

(b) a risk management strategy;

(c) a risk-management function dedicated to the framework;

(d) a management information system to support the effectiveness of the framework;

(e) a robust review process to ensure that the framework remains effective.

Note For the requirement for the governing body to approve the business plan, see rule 3.1.14 (1) (a).

7.1.3 What is risk management?

Risk management, for an authorised firm, includes some or all of the following, according to the nature, scale and complexity of the firm's business:

(a) identifying, assessing and reporting risk management information (including information dealing with issues of corporate strategy, mergers and acquisitions, and major projects and investments) to the firm's governing body and the firm's senior executive function and senior management in a timely way;

(b) assessing risk positions, risk exposures, the steps being taken to manage them and, if appropriate, pre-defined risk limits;

(c) participating in the process of approving new products or significant changes to existing products;

(d) preparing periodic reports to the firm's governing body setting out an overview of risk management during the relevant period, sending a copy of each such report to the firm's internal auditor and making the report available to the firm's external auditors;

(e) assessing risk events and identifying appropriate remedial action;

(f) assessing changes in the firm's risk profile;

(g) identifying available resources to manage the firm's risks;

(h) facilitating business continuity planning and disaster recovery for the firm;

(i) developing and maintaining external relationships relevant to risk management in the firm;

(j) developing and maintaining effective risk management communication within the firm;

(k) monitoring and assessing the adequacy and effectiveness of the firm's risk management policies, procedures and controls.

Guidance

Other rules may contain specific requirements as to risk management for firms authorised to carry on particular regulated activities. In particular, operational risk is of particular importance to banking business firms and Islamic banking business firms. (For the meaning of *operational risk*, see BANK, rule 7.1.1 (2) and IBANK, rule 7.1.1 (2).) For the management of operational risk in banking business firms, see BANK, Part 7.2, and in Islamic banking business firms, see IBANK, Part 7.2.

7.1.4 What is the risk management framework?

An authorised firm's ***risk management framework*** is the totality of systems, structures, policies, processes and people within the firm that identifies, measures, evaluates, monitors, reports on and controls or mitigates all internal and external sources of material risk. ***Material risks*** are risks that could have a material effect, financial or non-financial, on the firm, on its stakeholders or on the interests of its customers.

7.1.5 Risks to be addressed

An authorised firm's risk management framework must address, at least, the following risks (where they are material to the firm's operations):

(a) credit or asset risk;

(b) liquidity risk;

(c) market/investment risk;

(d) operational risk;

(e) strategy and planning risk;

(f) technology risk;

(g) market conduct risk;

(h) money laundering and terrorism financing risk;

(i) compliance, legal, reputational and regulatory risk;

(j) insurance underwriting;

(k) any other risks that, singly or in combination, could have a significant effect on the firm.

7.1.6 Risk appetite statement

(1) An authorised firm must have a documented risk appetite statement. A ***risk appetite statement*** is a high-level qualitative statement that clearly captures the firm's attitude to, and its level of acceptance of, different risks.

(2) The firm's ***risk appetite*** is the aggregate level and types of risk that the firm is willing to assume to achieve its strategic objectives and business plan. In setting its risk appetite, the firm must not breach its obligations or constraints determined by regulatory capital requirements, or liquidity or other needs.

(3) If appropriate, the statement must specify quantitative measures.

(4) The firm's governing body must review and approve the statement annually.

Guidance

The qualitative and quantitative measures referred to in this rule should reflect those expressed in the firm's risk management strategy (see rule 7.1.7 (2) (c)).

7.1.7 Risk management strategy

(1) An authorised firm's risk management strategy must be appropriate to the nature, scale and complexity of the firm's business.

(2) The strategy:

(a) must provide for assessing material risks;

(b) must set out policies and procedures for monitoring, prioritising and managing major risk exposures;

(c) must include both quantitative and qualitative considerations; and

(d) must provide for monitoring significant changes to the firm's risk profile.

(3) The strategy must include:

(a) objectives, principles and allocation of responsibility for dealing with risk across the firm, including any branches;

(b) defining and categorising the types of risk to which the firm is exposed;

Guidance

A suggested framework for the definition and categorisation of risks is set out in Schedule 1. The Regulatory Authority will use that framework in its approach to the assessment of risks posed by authorised firms, and the management of those risks. An authorised firm may either adapt this framework to reflect the nature, scale and complexity of its operations, or develop and implement its own risk classification framework.

(c) processes (covering contingency planning, business continuity, crisis management and fraud) for identifying, assessing, monitoring, managing and reporting on risks;

(d) a process for obtaining and recording the governing body's approval for any material change to, or deviation from, the strategy; and

(e) a process for obtaining a direction by the governing body settling any major question of the interpretation of the strategy.

(4) The firm must ensure that the strategy:

(a) is recorded in writing;

(b) is kept up to date to take into account new internal and external circumstances; and

(c) is reviewed at least once in every year.

(5) If the firm is part of a corporate group, the firm's governing body must know the implications for the firm of any group-wide risk management strategy.

7.1.8 Firms must provide appropriate training

The firm's senior management must ensure that appropriate risk management training is available to individuals at all levels throughout the firm. The training that is provided to an individual must be appropriate to the seniority, role and responsibilities of the individual.

7.1.9 Independence of certain employees

(1) An authorised firm must ensure that each employee who is allocated responsibilities within the firm's risk management framework is sufficiently free from influence for the framework to be effective in achieving its purposes.

(2) The requirement in subrule (1) is satisfied if reasonable measures have been taken to ensure that:

(a) no such employee is remunerated in a way that would tend to undermine his or her independence and objectivity in performing the duties;

Note For the requirements relating to a firm's remuneration policy, see rule 3.1.16.

(b) no such employee is involved in performing a function that generates, or is intended to generate, revenue for the firm;

(c) no such employee is limited or restricted as to the matters that he or she can investigate or report on in the exercise of his or her function;

(d) the reports and conclusions of such an employee can be honest and candid, without fear of reprisal; and

(e) pressure or influence is not applied to such an employee to modify his or her reports or conclusions.

Chapter 8 Outsourcing

Note for Chapter 8

Under this Chapter, the governing body of a firm is responsible for the firm's outsourcing policy (see rule 8.1.3) and the firm's senior management is responsible for implementing that policy (see rule 8.2.2).

Part 8.1 Outsourcing generally

8.1.1 Application of Chapter 8

This Chapter does not apply to the outsourcing of a function by an authorised firm if the functions are outsourced by the firm under COLL, PRIV or CAPI.

Note Each of COLL, PRIV and CAPI contains separate outsourcing rules for the outsourcing of functions by authorised firms to which those rules apply.

8.1.2 Meaning of *outsourcing*

In these rules:

outsourcing, for an authorised firm, means any arrangement that involves the firm relying on a separate service provider (including a member of the firm's corporate group) for the exercise of a function that relates to a regulated activity of the firm and would otherwise be exercised by the firm, but does not include the following arrangements:

(a) arrangements to provide advisory services (such as the provision of legal advice), audit services, personnel training services, billing services, and physical security;

(b) supply arrangements and functions (including, for example, the supply of electricity or water and the provision of catering and cleaning services);

(c) the purchase of standardised services (such as, for example, market information services and the provision of prices);

(d) the appointment of a group employee to exercise a controlled function for the firm.

8.1.3 Obligation to have outsourcing policy

(1) An authorised firm's governing body must establish and maintain an outsourcing policy.

(2) The policy must at least provide for:

(a) whether the firm will outsource any function at all; and

(b) what functions may be outsourced.

Note Appropriate records must be kept of policies and procedures — see GENE, rule 6.1.1.

(3) A policy that the firm will not outsource any function satisfies subrule (1).

(4) The governing body must review, at least once in every 2 years, the firm's outsourcing policy and procedures, including:

(a) its procedures for:

(i) assessing the feasibility of a proposed outsourcing and the risks that the outsourcing poses to the firm's business; and

(ii) costing any proposed material outsourcing; and

Note ***Material outsourcing*** is defined in rule 8.2.1.

(b) the criteria for selecting service providers.

(5) In this rule and rule 8.1.4, a reference to a firm's governing body is a reference to the board, membership, committee, body (whatever it is called) or individual (however the responsibility might have been delegated) that has responsibility for the outsourcing policy.

Examples for subrule (5)

For a firm that is part of a corporate group, the governing body that might have responsibility for outsourcing policy might be:

- a committee that is responsible for the place where the firm is located
- the firm's senior executive function
- any other body or person that has such responsibility.

8.1.4 Responsibility for outsourced functions

(1) The outsourcing of a function by an authorised firm does not relieve the firm's governing body from any obligation in relation to the function under the law applicable in the QFC.

(2) The governing body remains responsible for ensuring:

(a) that all requirements are complied with in relation to the function; and

(b) that the function is otherwise properly exercised.

(3) The governing body must exercise due skill, care and diligence in carrying out its obligations in relation to outsourced functions.

Note For the use of the term 'governing body' in this rule, see rule 8.1.3 (5).

8.1.5 Outsourcing arrangements

(1) An authorised firm may enter into an outsourcing arrangement only if:

(a) the firm's governing body has approved the firm's outsourcing policy; and

(b) the arrangement:

(i) is permitted by the policy;

(ii) will not reduce the firm's ability to fulfil its obligations to depositors, policyholders, clients and other stakeholders;

(iii) will not increase the firm's risk of non-compliance with the law applicable in the QFC or any other applicable law; and

(iv) will not affect the Regulatory Authority's ability to appropriately supervise the firm.

Example for paragraph (c) (iii)

The place where the service provider is located, or that place's legal system, could prevent the Authority from appropriately supervising the firm.

(2) The outsourcing arrangement must be in writing.

8.1.6 Review of outsourcing of controlled functions

(1) This rule applies if an authorised firm outsources the exercise of a controlled function.

(2) The senior management of the firm must review the arrangements for the outsourcing every year, to ensure that the independence, objectivity and effectiveness of the exercise of the function are not adversely affected.

(3) The senior management must report the results of the review to the firm's governing body.

Note The outsourcing of a function by an authorised firm does not relieve the firm from any obligation in relation to the function (see rule 8.1.4 (1)). The firm's governing body is ultimately responsible for ensuring that the firm carries out the firm's obligations under these rules (see rule 1.2.1).

Part 8.2 Material outsourcing arrangements

8.2.1 Meaning of *material outsourcing*

In these rules:

material outsourcing, for an authorised firm, means the outsourcing of a function of such importance that weakness or failure in the exercise of the function would cast serious doubt on:

(a) the firm's ability to comply with:

(i) any regulations, rules or principles; or

(ii) any condition, restriction or requirement of its authorisation;

(b) its financial performance or position; or

(c) its ability to continue in business.

Note The outsourcing of the internal audit function is a material outsourcing — see rule 6.4.2 (3).

8.2.2 Due skill in material outsourcing arrangements

(1) The senior management of an authorised firm must exercise due skill, care and diligence in selecting, entering into, managing and exiting from a material outsourcing arrangement.

(2) Before entering into a material outsourcing arrangement, the senior management:

(a) must assess the risks that the outsourcing poses to the firm's business; and

(b) must satisfy themselves that the service provider selected has the ability and capacity to perform the relevant function reliably and professionally at the start and during the life cycle of the outsourcing.

(3) For this rule, the senior management must take into account at least the following matters:

(a) whether the service provider is regulated, to what extent, and by whom;

(b) whether the function is subject to specific regulation or supervision;

(c) the risk that the service provider's service may become unavailable because of the number of other persons using the service provider;

(d) the financial stability and expertise of the service provider;

(e) any conflict of interest that might arise from the provision of the function by the service provider.

8.2.3 Written agreement for material outsourcing arrangements

(1) The written agreement (required by rule 8.1.5 (2)) between an authorised firm and a service provider for a material outsourcing arrangement must require the service provider:

(a) to deal with the Regulatory Authority in an open and co-operative way in relation to matters relating to the firm under the material outsourcing; and

(b) to grant the Authority access to the firm's books, records and data in the possession or control of the service provider.

Guidance

The Authority expects firms to be able to demonstrate that the outsourced function is being performed effectively. The Authority may seek documentary evidence relating to the performance of the service provider.

(2) The agreement must include, if appropriate, provisions as to:

(a) the law applicable to the agreement;

(b) the reporting or notification requirements on the service provider and the means for measuring quantitative and qualitative performance by the service provider;

(c) access by the firm, its internal auditors, external auditors or actuaries to the firm's books, records and data while they are in the possession or control of the service provider;

(d) the obligation to protect confidential information and personal data (that is, any information relating to an individual who can be identified, directly or indirectly, in particular by reference to an identification number or to 1 or more factors specific to the individual's physical, physiological, mental, economic, cultural or social identity);

(e) the rules for subcontracting, if the arrangement permits it;

(f) the termination rights of each party; and

(g) contingency arrangements.

Note Rule 8.2.6 requires contingency arrangements to be made to allow the business of the firm to continue in the event of a significant loss of services from the service provider.

8.2.4 Regulatory Authority to be notified of certain matters

(1) An authorised firm must not enter into a material outsourcing arrangement unless it gives the Regulatory Authority at least 30 business days' prior written notice of its intention to enter into the arrangement.

(2) If the arrangement permits subcontracting to a third party, the firm must give the Authority notice of that fact.

8.2.5 Additional information about material outsourcing arrangements

(1) The Regulatory Authority may, by written notice to an authorised firm, require the firm to give the Authority, within a stated reasonable period, information about a material outsourcing arrangement (or proposed material outsourcing arrangement) that the Authority reasonably needs to enable it to decide whether the arrangement complies with this Chapter.

(2) The power given by this rule is additional to the Authority's other powers.

Note See for example FSR, article 48 (Powers to obtain documents and information).

8.2.6 Contingency arrangements

(1) An authorised firm that enters into a material outsourcing arrangement must make comprehensive contingency arrangements to allow its business to continue in the event of a significant loss of services from the service provider.

(2) The contingency arrangements must include:

(a) an exit strategy; and

(b) if appropriate, provision for partial exit and step-in.

(3) The contingency arrangements must cover at least the following:

(a) a significant loss of resources at the service provider;

(b) financial failure of the service provider;

(c) unexpected termination of the outsourcing arrangement.

Chapter 9 Islamic financial institutions

Part 9.1 Preliminary

9.1.1 Application of Chapter 9

This Chapter applies to all Islamic financial institutions.

9.1.2 Definitions for Chapter 9

In this Chapter:

AAOIFI means the Accounting and Auditing Organisation for Islamic Financial Institutions.

Islamic financial business means the business of carrying on 1 or more regulated activities in accordance with Shari'a.

Part 9.2 Policies, procedures, systems and controls

9.2.1 Policies — compliance with Shari'a

An Islamic financial institution must establish and implement policies to ensure that its business is conducted in accordance with Shari'a. The policies must include effective and comprehensive procedures to ensure that the firm complies with:

(a) Shari'a (in general and in relation to the requirements for Islamic financial contracts); and

(b) the fatwas, rulings and guidelines issued by its Shari'a supervisory board.

9.2.2 Policy and procedures manual for Islamic financial business

An Islamic financial institution must establish, implement and maintain a policy and procedures manual for Islamic financial business. The manual must address the following matters:

(a) how the compliance oversight function will be undertaken in relation to compliance with Shari'a;

(b) how the institution's Shari'a supervisory board will oversee and advise it in regard to the institution's business;

(c) how fatwas, rulings and guidelines of the Shari'a supervisory board will be recorded, disseminated and implemented and the internal Shari'a review undertaken;

(d) how disputes and differences of opinion between the Shari'a supervisory board and the institution's governing body in relation to Shari'a compliance will be addressed;

(e) the process for approving the internal policies, procedures, systems and controls to ensure that:

(i) the institution's business is conducted in accordance with Shari'a; and

(ii) information is disseminated to customers and investors appropriately;

(f) how conflicts of interest and potential conflicts of interest will be identified and managed.

9.2.3 Evaluation of information given to firm

An Islamic banking business firm's governing body must evaluate the suitability and effectiveness of the information and reports that it and the firm's senior management receive under this Chapter. The test of suitability and effectiveness is whether the information and reports are suitable for effectively overseeing and implementing the principles and requirements set out in this Chapter.

9.2.4 Stress-testing

In carrying out stress-testing and developing its stress-testing scenarios, an Islamic banking business firm must consider the IFSB's guiding principles on stress-testing for institutions offering Islamic financial services and the recommended standards for stress-testing issued by the Basel Committee on Banking Supervision.

Part 9.3 Shari'a supervisory boards

Division 9.3.A Appointment and operation of Shari'a supervisory boards

9.3.1 Composition of Shari'a supervisory board

(1) An Islamic financial institution must have a Shari'a supervisory board. The board must have at least 3 members.

(2) Each member must be capable of exercising strong and independent oversight of, and adequate objective judgment about, Shari'a-related matters.

9.3.2 Appointment etc of members of Shari'a supervisory board

(1) An individual must not be appointed as a member of an Islamic financial institution's Shari'a supervisory board unless the individual is suitable to exercise the functions of such a member.

(2) The following are not eligible for appointment as a member of the Shari'a supervisory board of an Islamic financial institution:

(a) a controller (within the meaning of GENE, rule 8.1.3 (1)) of the institution;

(b) a member of the institution's governing body.

(3) Any appointment, dismissal or other change of a member of the Shari'a supervisory board must be approved by the institution's governing body.

9.3.3 Assessing suitability of proposed members of Shari'a supervisory board

When the governing body of an Islamic financial institution is assessing an individual's suitability for appointment as a member of

the institution's Shari'a supervisory board, the governing body must take into account:

(a) the individual's good character (honesty, integrity, fairness and reputation);

(b) the individual's competence, diligence, capability and soundness of judgment; and

(c) anything else that the governing body considers relevant.

9.3.4 Assessing good character of proposed members of Shari'a supervisory board

In assessing an individual's good character for rule 9.3.3, an Islamic financial institution's governing body must consider:

(a) whether the individual:

(i) has ever been convicted of a criminal offence, particularly an offence relating to dishonesty, fraud or financial crime;

Note For the meaning of ***financial crime***, see the Glossary.

(ii) has been the subject of any adverse findings or any settlement in civil proceedings, particularly in connection with banking or other financial business, misconduct or fraud;

(iii) has been the owner, manager or director of a company, partnership or other entity that:

(A) has been refused registration, authorisation, membership or a licence to conduct a trade, business or profession; or

(B) has had that registration, authorisation, membership or licence revoked, withdrawn or terminated;

resulting in the individual being refused the right to carry on a trade, business or profession requiring such a licence, registration or other authorisation;

(iv) has been a director, partner or otherwise involved in the management of a business that has gone into receivership,

insolvency or compulsory liquidation while the individual was connected with that business or within 1 year after the individual's departure from it;

(v) has been dismissed or asked to resign, or has resigned, from employment or from a position of trust, fiduciary appointment or similar position because of questions about his or her honesty and integrity;

(vi) has ever been disqualified from acting as a director or serving in a managerial capacity because of wrongdoing; or

(vii) has not been fair, truthful and forthcoming in dealings with customers, superiors, auditors and regulatory authorities in the past and has been the subject of any justified complaint relating to regulated activities;

(b) whether the individual shows readiness and willingness to comply with the requirements and standards of the regulatory system in the QFC and other legal, regulatory, or professional requirements and standards;

(c) whether the individual (or any business in which he or she is a controlling shareholder or has a controlling interest or exercises significant influence) has been investigated and disciplined or suspended by a regulatory or professional body, a court or a tribunal, whether publicly or privately; and

(d) anything else that the governing body considers relevant.

9.3.5 Assessing competence of proposed members of Shari'a supervisory board

(1) To be suitable for appointment as a member of the Shari'a supervisory board of an Islamic financial institution, an individual must be able to demonstrate the competence and ability to understand:

(a) the technical requirements of the institution's business;

(b) the risks inherent in the institution; and

(c) the processes required to conduct the institution's operations effectively.

(2) In making the assessment required by subrule (1), the institution's governing body must consider:

(a) whether the individual has demonstrated, through qualifications and experience, the capacity to successfully undertake the responsibilities of the position;

(b) whether the individual is physically, mentally and emotionally fit to perform the duties of the position;

(c) whether the individual has a sound knowledge of the institution's business and the responsibilities of the position; and

(d) anything else that the governing body considers relevant.

Guidance

1 The Regulatory Authority expects an Islamic financial institution to carry out background checks, and to verify that a person to be appointed as a member of the institution's Shari'a supervisory board has at least the minimum qualifications and experience set out in Appendix 4 of IFSB 10: *Guiding Principles on Shari'a Governance Systems for Institutions offering Islamic Financial Services*.

2 So far as possible, such an institution should use the suitability criteria and factors in this Division when appointing an individual to exercise the Shari'a compliance function and internal Shari'a review function. In addition, such an individual is expected to have:

- adequate training in Shari'a
- additional qualifications in finance
- good communication skills to enable him or her to liaise and work effectively with the Shari'a supervisory board
- organisational skills.

9.3.6 Policy in relation to appointments etc to Shari'a supervisory boards

An Islamic financial institution must document its policy in relation to:

(a) how appointments, dismissals or changes to the institution's Shari'a supervisory board will be made;

(b) the process through which the suitability of the members will be considered; and

(c) the remuneration of the members.

9.3.7 Records of assessment of suitability of Shari'a supervisory board members

(1) An Islamic financial institution must retain a record, for each individual who is or has been a member of its Shari'a supervisory board, of:

(a) its assessment of the individual's suitability to be such a member; and

(b) the agreed terms of engagement of the individual as such a member.

(2) The record for a member must include:

(a) the factors that were taken into account when assessing the member's suitability;

(b) the qualifications and experience of the member;

(c) the basis upon which the institution considered that the member was suitable; and

(d) details of any other Shari'a supervisory boards of which the member is, or has been, a member.

(3) The institution must retain the record for a former member of its Shari'a supervisory board for at least 6 years after the date on which he or she ceased to be such a member.

9.3.8 Islamic financial institution's obligations to Shari'a supervisory board

(1) An Islamic financial institution must take reasonable steps to ensure that the members of its Shari'a supervisory board are independent of the institution, and not subject to any conflict of interest with it.

Guidance

An Islamic financial institution's Shari'a supervisory board can be considered independent only if none of its members has a blood or close relationship with the

institution, the institution's officers or related parties, that could interfere (or be reasonably perceived as interfering) with the exercise by the board of independent judgment.

(2) The institution and its employees:

(a) must give the Shari'a supervisory board any assistance that it reasonably requires to perform its duties;

(b) must give the board right of access at all reasonable times to relevant records and information;

(c) must not interfere with the board's ability to perform its duties; and

(d) must not provide false or misleading information to the board.

9.3.9 Information about Shari'a supervisory board to be given to Regulatory Authority

An Islamic financial institution must provide the Regulatory Authority, on the Authority's request, with information about the qualifications, skills, experience and independence of the members or proposed members of the institution's Shari'a supervisory board.

Division 9.3.B Shari'a supervisory board reports

9.3.10 Annual Shari'a supervisory board report

(1) An Islamic financial institution must commission, from its Shari'a supervisory board, an annual report that complies with AAOIFI Standards on Governance, GSIFI No 1.

(2) The institution must give the Regulatory Authority a copy of each such annual report within 3 months after the day the relevant financial year of the institution ends.

Example

If a financial year of an Islamic financial institution ends on 31 December in a year, the annual report of the institution's Shari'a supervisory board must be given to the Regulatory Authority before 1 April in the next year.

9.3.11 Other Shari'a supervisory board reports

An Islamic financial institution must ensure that its Shari'a supervisory board prepares all the reports required by AAOIFI Standards on Governance, GSIFI No 2.

Division 9.3.C Internal Shari'a reviews

9.3.12 Islamic financial institutions to carry out internal Shari'a reviews

(1) An Islamic financial institution must from time to time carry out an internal Shari'a review to assess the extent to which the institution complies with Shari'a and with the fatwas, rulings and guidelines issued by its Shari'a supervisory board.

(2) The interval between reviews must be determined by the institution's Sharia supervisory board, taking into account the nature, scale and complexity of the institution's business.

(3) The objective of such a review is to ensure that the governing body and senior management of the institution carry out their responsibilities in relation to Shari'a (as determined by the firm's Shari'a supervisory board).

(4) The review must be carried out, in accordance with the AAOIFI standards relating to Shari'a governance, by:

(a) the institution as part of its internal audit function; or

(b) an independent entity that is competent to do so.

Guidance

1 For the purposes of assessing the competency of personnel or entities that carry out the internal Shari'a review, the institution should consult the AAOIFI Standards on Governance (GSIFI No. 3) and Appendix 4 of IFSB 10: *Guiding Principles on Shari'a Governance Systems for Institutions offering Islamic Financial Services*.

2 IFSB 3 states that fatwas, rulings, pronouncements and resolutions issued by the Shari'a supervisory board should be strictly adhered to. A person should not be assigned to carry out an internal Shari'a review unless the person:

- is adequately trained in Shari'a compliance

- has a competent grasp of the review process.

(5) The results of each review (including any instance of non-compliance) must be documented, and the institution must ensure that any non-compliance is rectified, so far as possible.

(6) The function or entity that carried out the review or reviews during a period must report on its findings in time for the next meeting of the Shari'a supervisory board. If the function or entity did not conduct any review during the period preceding a meeting, it must notify the board of the fact.

9.3.13 Institution must give copy of report to Regulatory Authority

An Islamic financial institution must give the Regulatory Authority a copy of the report or reports prepared by the institution's Shari'a supervisory board. The report or reports must be given within 3 months after the day the relevant financial year of the institution ends.

Example

If a financial year of an Islamic financial institution ends on 31 December in a year, the report of the Shari'a supervisory board must be given to the Regulatory Authority before 1 April in the next year. The Shari'a supervisory board's compliance report usually forms part of the institution's Annual Financial Report, but there could also be a second more detailed report of the compliance work undertaken addressed specifically to the Regulatory Authority.

Part 9.4 Conduct of Islamic financial business

9.4.1 Other firms not to be held out as Islamic financial institutions

An authorised firm that is not an Islamic financial institution must not hold itself out as an Islamic financial institution.

9.4.2 Islamic financial institutions not to conduct other financial business etc

An Islamic financial institution:

(a) must not hold itself out as conducting financial business other than Islamic financial business; and

(b) must not carry on any regulated activity otherwise than in accordance with Shari'a.

9.4.3 Disclosure about Shari'a supervisory board

(1) An Islamic financial institution must disclose the information specified in subrule (2) to a person with whom or on behalf of whom the institution conducts (or proposes to conduct) Islamic financial business, if the person so requests.

(2) The information is:

(a) the names of the members of the institution's Shari'a supervisory board; and

(b) how, and how often, the institution conducts Shari'a reviews.

9.4.4 Disclosure by Islamic insurers

An Islamic financial institution that effects or carries out contracts of takaful must disclose in its financial statements:

(a) the matters set out in AAOIFI FAS 12, in the way required by AAOIFI FAS 12; and

(b) the matters set out in AAOIFI FAS 13.

Guidance

1 An important matter that an Islamic financial institution must disclose under AAOIFI FAS 13, as applied by rule 9.4.4 (b), is how the institution would treat an insurance deficit or surplus. Appendix B to AAOIFI FAS 13 provides some guidance as to how to treat a deficit or surplus.

2 That appendix states that there are a number of ways to treat a deficit, including:

(a) settling the deficit from the reserve of policyholders, if any;

(b) borrowing the amount of the deficit from the shareholders' funds or from others (and paying it back from future surpluses);

(c) asking the policyholders to meet the deficit pro rata; and

(d) increasing the future premium contribution of policyholders on a pro-rata basis.

3 That appendix also states that there are a number of ways to allocate a surplus, including:

(a) allocating the surplus to all policyholders, regardless of whether or not they have made claims on the policy during the relevant financial period;

(b) allocating the surplus only among policyholders who have not made any claims during that financial period;

(c) allocating the surplus among policyholders who have not made any claims and those who have made claims of amounts less than their insurance contributions, provided that the latter category of policyholders should receive only the difference between their insurance contributions and their claims during the financial period;

(d) allocating the surplus between policyholders and shareholders; and

(e) allocating the surplus in other ways.

Schedule 1 Guidance — classification of risks

(rule 7.1.7)

The following table sets out an example of a system of classifying the risks to which an authorised firm is exposed. An authorised firm is free to adapt this framework to reflect the nature, scale and complexity of its operations, or to develop and implement its own risk classification framework.

Item	Risk factor	Explanation
1	**Financial soundness**	
1.1	Capital adequacy	The risks arising from the nature of an authorised firm's capital position. These risks include risks arising from the firm's capital planning framework, the composition and quality of capital, the adequacy of capital to support the level of current and expected business activities, the adequacy of reserves and access to further capital.
1.2	Revenue/ profitability	The risks arising from the nature of the firm's earnings. These risks include risks arising from the adequacy of profitability, volatility of revenues and profitability and track record of performance against budget.
2	**Business strategy**	
2.1	Quality of business strategy and plan	The risks arising from the firm's overall strategy. These risks include risks arising from the quality of the strategic planning process, the achievability of the strategy, the implications of the strategy, particularly for risk appetite, and the track record of implementation.
2.2	Regulated activities offered	The risks arising from the characteristics of the firm's business activities, including the extent and complexity of those activities.

Item	Risk factor	Explanation
2.3	Types of clients	The risks arising from the characteristics of the firm's client base, including the types of clients (market counterparties, business customers, commercial customers and retail customers).
2.4	Types of products	The risks arising from the characteristics of the current products or services provided by the firm. These risks include the complexity, tenor and performance of the products.
2.5	Markets targeted	The risks arising from the markets targeted, including the location of clients and the nature and jurisdiction of overseas investments offered.
2.6	Sources of business and distribution channels	The risks arising from the nature of the current sources of business and distribution mechanisms used by the firm. These risks include risks arising from introductions by existing clients and the use of intermediaries and sourcing overseas customers.
3	**Market and operational**	
3.1	Market risk	The risks arising from the type and nature of market risk undertaken by the firm. These risks include risks arising from the firm's risk appetite, and the nature of market risk exposures involved in the firm's products and services.
3.2	Credit risk	The risks arising from the type and nature of credit risk undertaken by the firm. These risks include risks arising from the firm's risk appetite, the nature of counterparty exposures involved in the firm's products and services, its portfolio characteristics and the nature and extent of credit risk mitigation.
3.3	Operational risk	The risks arising from the type and nature of operational risk involved in the firm's activities. These risks include risks arising from direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

Item	Risk factor	Explanation
3.4	Liquidity risk	The risks arising from the type and nature of the firm's liquidity or asset and liability mix. These risks include risks arising from the firm's liquidity management framework and the composition of liquidity to allow funding of the firm's operational and financial obligations both day to day and in crisis situations.
3.5	Insurance underwriting	The risks arising from the type and nature of insurance underwriting risk undertaken by the firm. These risks include risks arising from the firm's risk appetite, the nature of insurance underwriting exposures involved in the firm's products and services and the nature and extent of reinsurance cover.
3.6	Legal risk	The risks arising from the type and nature of the firm's contractual agreements. These risks include risks arising from the risk that contracts may not be enforceable under applicable law.
4	**Organisation and regulation**	
4.1	Clarity of legal ownership and structure	The risks arising from the structure of the firm or corporate group. These risks include risks arising from the nature of the legal and ownership structure and openness of the group structure to regulators.
4.2	Controllers and group entities	The risks arising from the characteristics of the firm's controllers. These risks include risks arising from the jurisdiction and characteristics of shareholder controllers, directors, and nature of other group entities. The risks arising from the relationship between the firm and the rest of its corporate group. These risks include risks arising from management arrangements, reliance on centralised functions, financial health and activities of the wider group and financial and other dependencies on other group entities.

Item	Risk factor	Explanation
4.3	Nature and extent of home state laws, regulation and supervision	The risks arising from the content of applicable laws (such as statutory priority to local creditors), the level of regulation undertaken by another financial services regulator and the reliance that can be placed on the supervision of the firm by that regulator.
4.4	Political and economic environment in home jurisdiction	The risks arising from any instability in political or environmental factors in the firm's home jurisdiction. This (these?) risks include risks arising from terrorism, political sanctions or likelihood of natural disasters.
4.5	Relationship with regulators	The risks arising from any instability in political or environmental factors in the firm's home jurisdiction. This (these?) risks may include risks arising from terrorism, political sanctions or likelihood of natural disasters.
5	**Clients**	
5.1	Communications with clients and financial promotions	The risks arising from the nature of financial promotion and advertising practices employed by the firm.
5.2	Client assets	The risks arising from arising from the firm holding or controlling of clients' money and assets.
5.3	Client categorisation	The risks arising from customer classification and the documentation procedures.
5.4	Advice management and dealing	The risks arising from dealing and managing customer assets and the quality of advice (for example, suitability, customer understanding of risk and charges).
5.5	Disclosure and reporting	The risks arising from the nature of product literature issued by the firm and the terms of business, periodic statements and other documentation provided to clients.

Item	Risk factor	Explanation
6	**Conflicts management**	
6.1	Identification and management	The risks arising from the identification of potential and actual conflicts of interest and how the firm manages them.
6.2	Staff remuneration	The risks arising from the recruitment quality and training procedures for the sales force. The risks arising from the nature of the remuneration scheme for employees.
6.3	Personal account dealings	The risks arising from potential insider dealing and the process for identifying and approving directors and employees trading for their personal accounts.
7	**Management and controls**	
7.1	Allocation of responsibilities	The risks arising from the nature of the allocation and definition of directors' and management responsibilities and the mechanism for ensuring that responsibilities are effectively delegated and carried out.
7.2	Quality of management and corporate governance	The risks arising from the quality of the firm's management, the nature of the firm's corporate governance and its overall compliance culture. These risks include risks arising from management's experience and integrity, fit with the business and operation of the executive body, non-executive directors and board committees.
7.3	Reporting lines and segregation	The risks arising from reporting lines between management and the board or other senior staff and the appropriate segregation of duties between functions of a risk-taking nature and those of a risk-management nature.
7.4	Compliance function arrangements	The risks arising from the nature and effectiveness of the compliance function. These risks include risks arising from its mandate, structure, staffing, methodology, reporting lines and effectiveness.

Item	Risk factor	Explanation
7.5	Risk management function arrangements	The risks arising from the nature and effectiveness of the risk management function. These risks include risks arising from its mandate, structure, staffing, methodology, reporting lines and effectiveness.
7.6	Risk management systems	The risks arising from the nature and effectiveness of the systems and procedures to identify, measure, monitor and control the risk of the business in an appropriate and timely manner. These risks include credit risk, insurance underwriting risk, market risk, operational risk, legal risk and new product risk.
7.7	Internal audit function arrangements	The risks arising from the nature and effectiveness of the internal audit function. These risks include risks arising from its mandate, structure, staffing, methodology, reporting lines and effectiveness.
7.8	Complaints arrangements	The risks arising from the firm's procedures to deal with the receipt of complaints and to consider complaints to rectify systemic issues.
7.9	Business continuity	The risks arising from the nature and effectiveness of business continuity arrangements. These risks include risks arising from the adequacy of the planning process, the quality of the business continuity plan and the testing process.
7.10	Outsourcing	The risks arising from the use of outsourcing. These risks include risks arising from the reliance on, and the controls over, the service provider. Authorised firms will need to be able to demonstrate that the systems and controls of service providers in relation to cybersecurity are at least as strong as the firm's own controls.
7.11	Monitoring and audit	The risks arising from the nature and effectiveness of the internal audit function. These risks include risks arising from its mandate, structure, staffing, methodology and effectiveness.

Item	Risk factor	Explanation
7.12	Employees and training	The risks arising from human resources issues. These risks include risks arising from recruitment, training, remuneration, disciplinary procedures and resources.
7.13	Provision of information to management	The risks arising from the nature of management information. These risks include risks arising from its adequacy, accuracy, relevance and timeliness and the effectiveness and efficiency of its distribution.
7.14	Data protection	The risks arising from the firm's use of personal information.
8	**Financial crime**	
8.1	Anti-money laundering procedures	The risks arising from the nature and effectiveness of the money laundering controls. These risks include risks arising from the effectiveness of the MLRO, training, identification of clients, know your business, internal and external reporting arrangements and record keeping arrangements.
8.2	Prevention of market abuse and financial crime	The risks arising from the firm's susceptibility to having market abuse carried out through it. These risks include risks arising from measures to prevent abusive, fraudulent or dishonest trading practices and co-operation in market enforcement matters.
9	**Human and technical resources**	
9.1	Approved individuals	The risks arising from the firm's susceptibility to having market abuse conducted through it. These risks include risks arising from measures to prevent abusive, fraudulent or dishonest trading practices and co-operation in market enforcement matters.
9.2	IT Systems and technical resources	The risks arising from the controls over the IT infrastructure. These risks include risks arising from adequacy of resources, procedures for implementation and procurement, effectiveness of security framework, etc. and consideration as to whether the IT infrastructure is an adequate platform on which to run the business.

Item	Risk factor	Explanation
9.3	Cybersecurity	The risk that the firm may not have the capacity to anticipate, detect and recover from cybersecurity attacks.
10	**Environmental and social impact**	
10.1	Impact of the firm's operations	The risk that the firm's operations may have a detrimental environmental effect or social effect.
10.2	Financial risk linked to climate change	The risk of financial loss arising from climate change, both physical risks (that is, relating to specific weather events, and shifts in climate) and transition risks (that is, the risks that may arise from the process of adjustment towards a lower-carbon economy).

Glossary

(see rule 1.1.3)

actuarial function has the meaning given by rule 1.2.15.

AML/CFTR means the *Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019*.

AMLG means the *Anti-Money Laundering and Combating the Financing of Terrorism (General Insurance) Rules 2019*.

approved actuary of a QFC insurer means the individual who is approved to exercise the actuarial function for the insurer.

approved individual means an individual who is approved under FSR, article 41, to exercise 1 or more controlled functions.

authorisation means an authorisation granted under FSR, Part 5.

authorised firm (or ***firm***) means a person that has been granted an authorisation in accordance with FSR, Part 5.

BANK means the *Banking Business Prudential Rules 2014*.

board of directors (or ***board***) of an authorised firm that is incorporated in the QFC has the meaning given by rule 3.3.3.

business day means a day that is not a Friday, Saturday, or a public or bank holiday in Qatar.

branch means the local office in the QFC of a company or limited liability partnership that is incorporated in a jurisdiction outside the QFC.

CAPI means the *Captive Insurance Business Rules 2011*.

category A firm has the meaning given by rule 3.3.2.

category B firm has the meaning given by rule 3.3.2.

COLL means the *Collective Investment Schemes Rules 2010*.

company means:

(a) a company that is incorporated under the Companies Regulations; or

(b) a legal person that is incorporated under the law of a jurisdiction outside the QFC, in which the liability of each member (in its

capacity as a member) is limited to the amount of the member's contribution to the company's capital.

Companies Regulations means the *Companies Regulations 2005* of the QFC.

compliance oversight function has the meaning given by rule 1.2.13.

contract of insurance means the specified product described in FSR, Schedule 3, Part 3, paragraph 10.

controlled function has the meaning given by rule 1.2.5 (2).

corporate governance framework has the meaning given by rule 1.2.2.

corporate group: an entity's corporate group is made up of:

(a) the entity itself;

(b) any parent entity of the entity; and

(c) any subsidiary (direct or indirect) of that entity or of any parent entity of the entity.

director of an authorised firm that is incorporated in the QFC has the meaning given by rule 3.3.3.

document means a record of information in any form (including electronic form), and includes, for example:

(a) anything in writing or on which there is writing; and

(b) anything on which there are figures, marks, numbers, perforations, symbols or anything else having a meaning for individuals qualified to interpret them; and

(c) a drawing, map or photograph or plan; and

(d) any other item or matter (in whatever form) that is, or could reasonably be considered to be, a record of information.

employee: an individual is an ***employee*** of a person (the ***employer***) if:

(a) the individual is employed or appointed by the employer in connection with the employer's business, whether under a contract of service or for services or otherwise; or

(b) the employee's services are placed at the employer's disposal, and under the employer's control, under an arrangement between the employer and a third party.

entity means any kind of entity, and includes, for example, any person.

executive governance function has the meaning given by rule 1.2.6.

exercise a function includes perform the function.

finance function has the meaning given by rule 1.2.9.

financial crime means the use of the financial system in the QFC for criminal, fraudulent or dishonest purposes, including, for example, insider trading, market abuse, handling the proceeds of crime, money laundering and terrorist financing.

firm (or ***authorised firm***) means a person that has been granted an authorisation in accordance with FSR, Part 5.

FSR means the *Financial Services Regulations* of the QFC.

function includes power.

GENE means the *General Rules 2005*.

governing body of an authorised firm has the meaning given by rule 1.2.1.

IBANK means the *Islamic Banking Business Prudential Rules 2015*.

IFSB means the Islamic Financial Services Board.

independent non-executive director of an authorised firm has the meaning given by rule 3.3.4.

INDI means the *Individuals (Assessment, Training and Competency) Rules 2014*.

INMA means the *Investment Management and Advisory Rules 2014*.

insurer (or ***QFC insurer***) means an authorised firm that has an authorisation to conduct insurance business.

insurance business has the meaning given by PINS, rule 1.2.4.

internal auditor means:

(a) in the case of an authorised firm that has an individual who is approved to exercise the internal audit function — that individual; and

(b) in the case of a QFC insurer that does not have such an individual — the firm of auditors appointed in accordance with paragraph 6.4.2 (2) (b).

internal audit function has the meaning given by rule 1.2.14.

internal control and assurance function has the meaning given by rule 1.2.4 (2).

internal controls and assurance framework has the meaning given by rule 1.2.4.

Islamic financial institution means an authorised firm whose authorisation includes a condition that the whole of the firm's business must be conducted in accordance with Shari'a.

limited liability partnership means a partnership:

(a) that is incorporated under the LLP Regulations; or

(b) that is incorporated under the law of a jurisdiction outside the QFC by which the liability of each partner (in its capacity as a partner) is limited to the amount of the partner's contribution to the partnership's capital.

LLP Regulations means the *Limited Liability Partnerships Regulations 2005* of the QFC.

material outsourcing has the meaning given by rule 8.2.1.

MLRO function has the meaning given by rule 1.2.11.

month means calendar month — that is, the period beginning at the start of any day of one of the 12 named months of the year and ending:

(a) at the end of the day before the corresponding day on the next named month; or

(b) if there is no corresponding day — at the end of the last day of next named month.

non-executive director of an authorised firm has the meaning given by rule 3.3.4.

non-executive governance function has the meaning given by rule 1.2.7.

outsourcing has the meaning given by rule 8.1.2.

person means:

(a) an individual (including an individual occupying an office or position from time to time); or

(b) a legal person — that is, an entity, other than an individual, on which the legal system of a jurisdiction confers rights and imposes duties (including, for example, any entity that can own, deal with or dispose of property).

PINS means the *Insurance Business Rules 2006*.

PRIV means the *Private Placement Schemes Rules 2010*.

QFC means the Qatar Financial Centre.

QFC bank means an authorised firm that is:

(a) a deposit-taker, within the meaning of BANK; or

(b) an Islamic bank or Islamic investment dealer, within the respective meanings of IBANK.

QFC captive insurer has the meaning given by CAPI, rule 1.2.1.

QFC entity means either:

(a) a company incorporated under the Companies Regulations; or

(b) a limited liability partnership incorporated under the LLP Regulations.

QFC insurer (or ***insurer***) means an authorised firm that has an authorisation to conduct insurance business.

regulated activity means an activity that is a regulated activity under FSR.

Regulatory Authority means the Qatar Financial Centre Regulatory Authority established under Law No. (7) of 2005 of the State of Qatar, article 9.

related: a person (the ***second person***) is related to another person (the ***first person***) if:

(a) the second person is a subsidiary, associate or holding company of the first person;

(b) the second person is a subsidiary or associate of the holding company of the first person;

(c) the second person is a director or officer of the first person, or of a person related to the first person because of paragraph (a) or (b);

(d) the second person is the spouse or minor child of an individual mentioned in paragraph (c);

(e) the second person is a company that is a subsidiary of, or subject to significant influence by or from, an individual mentioned in paragraph (c) or (d).

risk appetite for an authorised firm has the meaning given by rule 7.1.6 (2).

risk appetite statement has the meaning given by rule 7.1.6 (1).

risk management framework has the meaning given by rule 1.2.3**.**

risk management function has the meaning given by rule 1.2.12.

risk management strategy has the meaning given by rule 7.1.4.

senior executive function has the meaning given by rule 1.2.8.

senior management of an authorised firm has the meaning given by rule 4.1.1.

senior management function has the meaning given by rule 1.2.10.

Shari'a supervisory board, of an authorised firm, means the board appointed for the firm under rule 9.3.1.

specified product means a product that is a specified product under FSR, Schedule 3, Part 3.

subsidiary: an entity is a subsidiary of another entity if that other entity is the parent entity of the first entity.

writing means any form of writing, and includes, for example, any way of representing or reproducing words, numbers or symbols or

anything else in legible form (for example, by printing or photo-copying).

year means a year of the Gregorian calendar.

Endnotes

1 Abbreviation key

a	=	after	ins	=	inserted/added
am	=	amended	om	=	omitted/repealed
amdt	=	amendment	orig	=	original
app	=	appendix	par	=	paragraph/subparagraph
art	=	article	prev	=	previously
att	=	attachment	pt	=	part
b	=	before	r	=	rule/subrule
ch	=	chapter	renum	=	renumbered
def	=	definition	reloc	=	relocated
div	=	division	s	=	section
g	=	guidance	sch	=	schedule
glos	=	glossary	sdiv	=	subdivision
hdg	=	heading	sub	=	substituted

2 Rulebook history

Governance and Controlled Functions Rules 2020

made by

Governance and Controlled Functions Rules 2020 (QFCRA Rules 2020-4)
Made 8 July 2020
Commenced 1 July 2021
Version No. 1

3 Amendment history