هيئة تنظيم
مركز قطر للمال
QATAR FINANCIAL CENTRE
REGULATORY AUTHORITY

Islamic Banking Business Prudential (Operational Risk) Amendments Rules 2020

QFCRA Rules 2020-3

The Board of the Qatar Financial Centre Regulatory Authority makes the following rules, and gives the following guidance, under the *Financial Services Regulations*.

Dated 8 July 2020.

Mohammed bin Hamad bin Qasim Al Thani
Deputy Chairman

Islamic Banking Business Prudential (Operational Risk) Amendments Rules 2020

QFCRA Rules 2020-3

made under the

Financial Services Regulations

Contents

1 Name of rules

These rules are the *Islamic Banking Business Prudential (Operational Risk) Amendments Rules 2020*.

2 Commencement

These rules commence on 1 January 2021.

3 Amendment

These rules amend the *Islamic Banking Business Prudential Rules 2015*.

4 Explanatory notes

An explanatory note in these rules is not part of these rules.

Schedule 1 Amendments

(see rule 3)

[1.1] Rule 1.1.14, note 2

omit

CTRL, rule 4.1.4.

insert

CTRL.

Explanatory note

This amendment omits a cross-reference to a specific provision of CTRL (which is shortly to be replaced).

[1.2] Rule 1.2.11, note, 6th dot-point

substitute

- operational risk—see rule 7.2.1

Explanatory note

This amendment and the next correct cross-references to provisions of Chapter 7 after the substitution of the new chapter by item 0.

[1.3] Rule 3.2.1 (2), note

substitute

Note For how to calculate the firm's market risk and operational risk capital requirements, see rule 6.1.1 (3) and Part 7.4, respectively.

[1.4] Chapter 7

substitute

Chapter 7 Operational risk

Part 7.1 Principles

7.1.1 Introduction

(1) This Chapter sets out:

(a) the requirements for an Islamic banking business firm's operational risk management policy to identify, measure, evaluate, manage and control or mitigate operational risk;

(b) the requirements for the firm to collect data on losses caused by operational risk events; and

(c) how to calculate the firm's operational risk capital requirement.

Note The firm's operational risk capital requirement is part of its risk-based capital requirement—see rule 3.2.5.

(2) ***Operational risk*** is the risk resulting from inadequate or failed internal processes, people and systems, or from external events. Operational risk includes legal risk and Shari'a non-compliance risk but does not include strategic risk or reputational risk.

(3) ***Legal risk***, of an Islamic banking business firm, includes exposures to fines, penalties or punitive damages resulting from supervisory actions as well as private settlements.

(4) Legal risk can arise from:

(a) the firm's operations (that is, from legal risks common to all financial institutions); or

(b) problems of legal uncertainty in interpreting and enforcing contracts based on Shari'a.

Note For examples of the operational risks that may arise from Islamic financial contracts, see Part 7.4.

(5) Legal risk also includes the risk that *sukuk* in which the firm is the originator, sponsor or manager fail to perform as intended because of a legal deficiency.

(6) ***Shari'a non-compliance risk*** is the risk to an Islamic banking business firm of non-compliance resulting from the failure of the firm's Shari'a compliance policy to ensure that Shari'a rules and principles (as determined by its Shari'a supervisory board) are complied with.

Guidance

1 Shari'a non-compliance risk can lead to non-recognition of an Islamic banking business firm's income, and resultant losses. For *sukuk*, the risk may adversely affect the marketability (and, therefore, the value) of the *sukuk*.

2 Shari'a non-compliance risk can take 2 forms:

- the risk relating to potential non-compliance with Shari'a rules and principles in the firm's operations, including the risk that non-permissible income is recognised; and
- the risk relating to the firm's fiduciary responsibilities as *mudarib* towards fund providers under a *mudarabah* contract, according to which, in the case of negligence, misconduct, fraud or breach of contract by the *mudarib*, the funds provided by the fund providers become a liability of the *mudarib*.

3 Although the operational risk that could arise for Islamic banking business firms can be considered similar to that of conventional banks, the characteristics of such risk may be different, thus:

- Shari'a-compliant products may involve processing steps different from those of their conventional counterparts
- the assets held on the balance sheets of Islamic banking business firms (physical assets and real estate) are different from those of conventional banks
- the requirements of Shari'a compliance result in different risks relating to information technology products and systems.

4 For examples of Shari'a requirements that must be complied with by an Islamic banking business firm in relation to Islamic financial contracts, see Part 7.5. Failure to comply with the requirements gives rise to Shari'a non-compliance risk.

Part 7.2 Principles of operational risk management

Note for Part 7.2

This Part sets out the requirement for Islamic banking business firms in relation to the management of operational risk. There are general requirements relating to risk management (including the management of operational risk) in CTRL, which apply to Islamic banking business firms in common with all other authorised firms.

7.2.1 Principle 1: risk management culture

The general obligations of an Islamic banking business firm's governing body and senior management under CTRL in relation to the firm's risk management culture include an obligation to establish a strong operational risk management culture. A general reference in CTRL to risk management includes the management of operational risk specifically.

7.2.2 Principle 2: operational risk management framework

(1) An Islamic banking business firm must develop, implement and maintain a framework for the management of operational risk that:

(a) is fully integrated into the firm's overall risk management processes; and

(b) is appropriate for the firm, taking into account the firm's nature, size, complexity and risk profile.

Guidance

The fundamental premise of sound risk management is that the firm's governing body and management understand the nature and complexity of the risks inherent in the firm's products, services and activities. This is particularly important for operational risk, given that operational risk is inherent in all business products, activities, processes and systems.

(2) The framework must be appropriately integrated into the risk management processes across all levels of the firm, including those at the group and business line levels, and into new business initiatives' products, activities, processes and systems. In addition, the results of the firm's operational risk assessment must be

incorporated into the firm's overall business strategy development processes.

Guidance

The framework is a vital means of understanding the nature and complexity of operational risk.

(3) The framework must be comprehensively and appropriately documented in policies approved by the firm's governing body, and must include definitions of operational risk and operational loss.

Guidance

An Islamic banking business firm that does not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of its framework.

(4) The firm's framework documentation:

(a) must clearly identify the governance structures used to manage operational risk, including reporting lines and accountabilities;

(b) must clearly describe the risk assessment tools and how they are used;

(c) must clearly describe the firm's accepted operational risk appetite and tolerance, its thresholds or limits for inherent and residual risk, and its approved risk mitigation strategies and instruments;

(d) must clearly describe the firm's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

(e) must establish risk reporting and management information systems;

(f) must provide a set of operational risk terms to ensure that risk identification, exposure rating and risk management objectives are consistent throughout the firm;

(g) must provide for appropriate independent review and assessment of operational risk; and

(h) must require the policies to be reviewed, and revised as appropriate, whenever a significant change occurs in the firm's operational risk profile.

7.2.3 Principle 3: governing body to approve framework

(1) The governing body of an Islamic banking business firm must establish, approve and periodically review the firm's operational risk management framework. The governing body must oversee the firm's senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

(2) The governing body:

(a) must establish a management culture, and supporting processes, to understand the nature and scope of the operational risk inherent in the firm's strategies and activities, and must develop comprehensive, dynamic oversight and control environments that are fully integrated into or coordinated with the overall framework for managing all risks across the firm;

(b) must provide senior management with clear guidance and direction regarding the principles underlying the framework and must approve the corresponding policies developed by senior management;

(c) must regularly review the framework to ensure that the firm has identified, and is managing, the operational risk arising from external market changes and other environmental factors, and the operational risks associated with new products, activities, processes or systems, including changes in risk profiles and priorities (for example changing business volumes);

(d) must ensure that the framework is subject to effective independent review by audit or other appropriately trained persons; and

(e) must ensure that, as best practice evolves, the firm's senior management avails themselves of those advances.

Guidance

Strong internal controls are a critical aspect of the management of operational risk, and the governing body should establish clear lines of management responsibility and accountability for implementing a strong control environment. The control environment should provide appropriate independence and separation of duties between operational risk management functions, business lines and support functions.

7.2.4 Principle 4: risk appetite and tolerance statement

(1) An Islamic banking business firm must approve and review its risk appetite and tolerance for operational risk.

(2) The firm must consider:

(a) all relevant risks;

(b) the firm's level of risk aversion;

(c) its current financial condition; and

(d) its strategic direction.

(3) The firm must set out the various operational risk appetites within the firm and must ensure that they are consistent. The firm must approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite and tolerance.

(4) The firm must regularly review the appropriateness of limits and the overall operational risk appetite and tolerance. Such a review must consider changes in the external environment, significant increases in business or activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume and nature of breaches of limits.

(5) The firm must monitor management's adherence to the statement and must provide for timely detection and remediation of breaches.

7.2.5 Principle 5: role of senior management

(1) The senior management of an Islamic banking business firm must develop, for approval by the firm's governing body, a clear, effective and robust governance structure for managing operational risk, with well defined, transparent and consistent lines of responsibility. The senior management is responsible for consistently implementing and maintaining, throughout the firm, policies, processes and systems for managing operational risk in all of the firm's products, activities, processes and systems consistently with the firm's risk appetite and tolerance.

(2) The firm's senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. The mechanisms should include systems to report, track and, when necessary, escalate issues to ensure that they are resolved.

(3) The firm's senior management must translate the operational risk management framework established by the governing body into specific policies and procedures that can be implemented and verified within the firm's business units. Senior management must clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and to ensure that the necessary resources are available to manage operational risk in line within the bank's risk appetite and tolerance statement.

(4) The firm's senior management must ensure that the management oversight process is appropriate for the risks inherent in each business unit's activity.

(5) The firm's senior management must ensure that the staff who are responsible for managing operational risk coordinate and communicate effectively with the staff who are responsible for:

(a) managing other risks (such as credit risk and market risk); and

(b) procuring external services (such as takaful risk transfer) and for making outsourcing arrangements.

Guidance

Failure to do so could result in significant gaps or overlaps in the firm's overall risk management program.

(6) The managers of the firm's corporate operational risk function must be of sufficient stature within the firm to perform their duties effectively.

Guidance

The standing within the firm of the managers of operational risk would ideally be evidenced by their titles being similar to those of the managers of other risk management functions such as the management of credit, market and liquidity risk.

(7) The senior management must ensure that the firm's activities are conducted by staff with the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the firm's risk policy must have authority independent from the units they oversee.

7.2.6 Principle 6: risk identification and assessment

(1) The senior management of an Islamic banking business firm must ensure that the operational risk inherent in all of the firm's products, activities, processes and systems is identified and assessed to make sure that the inherent risks and incentives are well understood.

Guidance

Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal factors and external factors. Sound risk assessment allows the firm to better understand its risk profile and allocate risk management resources and strategies most effectively. Tools that can be used for identifying and assessing operational risk include:

- ***audit findings***—although audit findings primarily focus on control weaknesses and vulnerabilities, they can also give insight into inherent risk that is due to internal or external factors
- ***internal loss data collection and analysis***—internal operational loss data provides meaningful information for assessing the firm's exposure to operational risk and the effectiveness of internal controls

- ***external data collection and analysis***—external data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at other organisations; external loss data can be compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures
- ***risk assessments***—in a risk assessment, often referred to as a *risk self-assessment*, the firm assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact; a similar approach, *risk control self-assessment* (RCSA), typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered); *scorecards* build on RCSAs by weighting residual risks to provide a means of translating RCSA output into metrics that give a relative ranking of the control environment
- ***business process mapping***—business process mappings identify the key steps in business processes, activities and organisational functions, and identify the key risk points in the overall business process; process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness, and can help prioritise subsequent management actions
- ***risk and performance indicators***—risk and performance indicators are risk metrics and statistics that provide insight into a firm's risk exposure; risk indicators, often referred to as *key risk indicators*, are used to monitor the main drivers of exposure associated with key risks; performance indicators, often referred to as *key performance indicators*, provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss; risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans
- ***scenario analysis***—scenario analysis is a process of obtaining expert opinion from business line and risk managers to identify potential operational risk events and assess their potential outcome; scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions; however, given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process
- ***measurement***—larger firms may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure; the results can be used in an

economic capital process and can be allocated to business lines to link risk and return

- ***comparative analysis***—that is, comparing the results of the various assessment tools to provide a more comprehensive view of the firm's operational risk profile; for example, comparison of the frequency and severity of internal data with RCSAs can help the firm determine whether self-assessment processes are functioning effectively; scenario data can be compared to internal and external data to gain a better understanding of the severity of the firm's exposure to potential risk events.

(2) The firm must ensure that its internal pricing and performance measurement mechanisms appropriately take into account operational risk.

Guidance

If operational risk is not considered, risk-taking incentives might not be appropriately aligned with the firm's risk appetite and tolerance.

7.2.7 Principle 7: approval process for new products etc

(1) The senior management of an Islamic banking business firm must ensure that there is an approval process that fully assesses operational risk for all new products, activities, processes and systems.

Guidance

In general, an Islamic banking business firm's operational risk exposure is increased when the firm engages in a new activity, develops a new product, enters an unfamiliar market, implements a new business process technology system or engages in a business distant from its head office. Moreover, the level of risk may increase when a new product, activity, process or system transition from an introductory level to a level that represents a significant source of revenue or a business-critical operation.

(2) An Islamic banking business firm must ensure that its risk management control infrastructure is appropriate at inception and that it keeps pace with the rate of growth of, or changes to, products, activities, processes and systems.

(3) An Islamic banking business firm must have policies and procedures that address the process for review and approval of new products, activities, processes and systems. The review and approval process must consider:

(a) the risks inherent in the new product, activity, process or system;

(b) changes to the firm’s operational risk profile and appetite and tolerance, including the risk of existing products or activities;

(c) the necessary controls, risk management processes and risk mitigation strategies;

(d) the residual risk;

(e) changes to relevant risk thresholds or limits; and

(f) the procedures and metrics to measure, monitor, and manage the risk of the new product, activity, process or system.

(4) The approval process must also include ensuring that appropriate investment has been made in human resources and technology infrastructure before a new product, activity, process or system is introduced.

(5) The implementation of new products, activities, processes and systems must be monitored to identify any significant differences to the expected operational risk profile, and to manage any unexpected risks.

7.2.8 Principle 8: monitoring and reporting

(1) The senior management of an Islamic banking business firm must implement a process to regularly monitor operational risk profiles and material exposures to losses. There must be appropriate reporting mechanisms at the board, senior management, and business line levels that support proactive management of operational risk.

(2) An Islamic banking business firm must ensure that its reports are comprehensive, accurate, consistent and actionable across business lines and products.

Guidance

Reports should be manageable in scope and volume; too much or too little data impedes effective decision-making. An Islamic banking business firm should endeavour to continuously improve its operational risk reporting.

(3) Reporting must be timely and the firm must be able to produce reports in both normal and stressed market conditions. The frequency of reporting must reflect the risks involved and the pace and nature of changes in the operating environment.

(4) The results of monitoring activities, and assessments of the framework by the firm's internal audit or risk management functions, must be included in regular management and board reports. Reports generated for the Regulatory Authority must also be reported internally to senior management and the board, where appropriate.

(5) Operational risk reports must include:

(a) breaches of the firm's risk appetite and tolerance statement, and breaches of thresholds or limits;

(b) details of recent significant internal operational risk events and losses; and

(c) relevant external events and any possible effect on the firm and operational risk capital.

Guidance

Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making.

(6) The firm must analyse its data capture and risk reporting processes periodically with a view to continuously improving the firm's risk management performance and advancing its risk management policies, procedures and practices.

7.2.9 Principle 9: control and mitigation

(1) The requirements of this rule are in addition to those set out in CTRL.

(2) In addition to separation of duties and dual control, an Islamic banking business firm must ensure that it has other traditional internal controls as appropriate to address operational risk.

Examples of controls

- clearly established authorities and processes for approval
- close monitoring of adherence to assigned risk thresholds or limits
- safeguards for access to, and use of, bank assets and records
- appropriate staffing level and training to maintain expertise
- ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations
- regular verification and reconciliation of transactions and accounts.

(3) An Islamic banking business firm must ensure that it has appropriate controls to manage technology risk.

Guidance

1 Effective use and sound implementation of technology can contribute to the control environment. For example, automated processes are less prone to error than manual processes. However, automated processes introduce risks that must be addressed through sound technology governance and infrastructure risk management programs.

2 The use of technology related products, activities, processes and delivery channels exposes an Islamic banking business firm to strategic, operational, and reputational risks and the possibility of material financial loss.

3 Sound technology risk management uses the same precepts as operational risk management and includes:

- governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the firm's business objectives
- policies and procedures that facilitate the identification and assessment of risk
- establishment of a risk appetite and tolerance statement and performance expectations to assist in controlling and managing risk
- implementation of an effective control environment and the use of risk transfer strategies that mitigate risk
- monitoring processes that test for compliance with policy thresholds or limits.

4 Mergers and acquisitions that result in fragmented and disconnected infrastructure, cost-cutting measures or inadequate investment can undermine the firm's ability to:

- aggregate and analyse information across risk dimensions or the consolidated enterprise
- manage and report risk on a business line or legal entity basis
- oversee and manage risk in periods of high growth.

5 The firm's management should make appropriate capital investment or otherwise provide for a robust infrastructure at all times, particularly before mergers are consummated, high growth strategies are initiated, or new products are introduced.

(4) The firm's governing body must decide the maximum loss exposure that the firm is willing, and has the financial capacity, to assume, and

must perform an annual review of the firm's risk and takaful management programme.

Guidance

If internal controls do not adequately address risk and exiting the risk is not a reasonable option, the firm can complement the controls by seeking to transfer the risk to another party such as through takaful.

Risk transfer is an imperfect substitute for sound controls and risk management programs. Therefore, the firm should view risk transfer as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms to quickly identify, recognise and rectify distinct operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as takaful truly reduce risk, transfer the risk to another business sector or area, or create a new risk (for example counterparty risk).

7.2.10 Principle 10: business resiliency and continuity

(1) An Islamic banking business firm must have business resiliency and continuity plans to ensure that the firm can continue to operate, and can limit its losses, in the event of severe business disruption.

Guidance

An Islamic banking business firm is exposed to disruptive events, some of which may be severe and result in an inability to fulfil some or all of the firm's business obligations. Incidents that damage or render inaccessible the firm's facilities, telecommunication or information technology infrastructures, or a pandemic event that affects human resources, can result in significant financial losses to the firm, and broader disruptions to the financial system.

(2) An Islamic banking business firm must establish business continuity plans commensurate with the nature, size and complexity of the firm's operations. The plans must take into account different likely or plausible scenarios to which the firm may be vulnerable.

(2) Continuity management must incorporate business impact analysis, recovery strategies, testing, training and awareness programs, and communication and crisis management programs. The firm must identify critical business operations, key internal and external dependencies, and appropriate resilience levels.

(3) Plausible disruptive scenarios must be assessed for their financial, operational and reputational impact, and the resulting risk assessment

must be the foundation for recovery priorities and objectives. Continuity plans should establish contingency strategies, recovery and resumption procedures, and plans for informing management, employees, the Regulatory Authority, customers, suppliers and, if appropriate, the civil authorities.

(4) The firm must periodically review its continuity plans to ensure that contingency strategies remain consistent with the firm's current operations, risks and threats, resiliency requirements, and recovery priorities. Training and awareness programmes must be implemented to ensure that the firm's staff can effectively carry out the plans.

(5) The firm must test each plan periodically to ensure that its recovery and resumption objectives and timeframes can be met. If possible, the firm must participate in disaster recovery and business continuity testing with key service providers.

(6) The results of testing must be reported to the firm's management and governing body.

7.2.11 Principle 11: disclosure

Note These rules do not yet have provisions on disclosure. Those provisions are to be inserted in the next phase of the development of these rules.

Part 7.3 Collection and reporting of operational loss data

7.3.1 Basic requirement—operational loss dataset

(1) An Islamic banking business firm must have documented procedures and processes to identify, collect and treat internal loss data for operational risk events. However, the firm need not collect data on any operational risk event for which the gross amount of loss is less than QR 40,000.

(2) In this Chapter, the set of data resulting from that collection is called the firm's ***operational loss dataset***.

(3) The procedures and processes:

(a) must be subject to validation before the dataset is used to calculate the firm’s operational risk capital requirement; and

(b) must be regularly independently reviewed by the firm’s internal or external audit functions.

(4) The procedures and processes must provide for the collection of at least the following information for an operational risk event:

(a) the gross amount of the resulting loss (the ***gross loss***);

(b) if available, the date when the event happened or began (***date of occurrence***);

(c) the date when the firm became aware of the event (***date of discovery***);

(d) the date (or dates) when the event resulted in a loss, reserve or provision against a loss being recognised in the firm’s profit and loss accounts (***date of accounting***);

(e) any recovery of the gross loss;

(f) descriptive information about the drivers or causes of the event.

(5) The level of detail of the information the firm collects about an event must be proportionate to the gross loss amount resulting from the event.

(6) When building the dataset, the firm must use the date of accounting as the date of a loss (except that, in the case of a legal loss event (that is, a legal event that results in a loss), the bank must use a date no later than the date of accounting).

(7) If 2 or more losses:

(a) had the same operational risk event in common as a cause; or

(b) were caused by related operational risk events over time, but were posted to the accounts over several years;

the losses must be allocated to the corresponding years of the loss database, in line with their accounting treatment.

(8) Data on losses that result from mergers or acquisitions must be included in the dataset.

(9) The following are not to be included in the dataset:

(a) costs of general maintenance on property, plant or equipment;

(b) internal or external expenditure to enhance the firm's business after operational risk losses (such as upgrades, improvements, risk assessment initiatives and enhancements);

(c) takaful fees or premiums.

7.3.2 Meaning of *gross loss*, *recovery* and *net loss* for operational risk events

(1) The ***gross loss*** for an operational risk event is the loss resulting from the event before any kind of recovery. Gross loss from such an event includes:

(a) any direct charge (including any impairment or settlement) to the relevant firm's profit and loss accounts;

(b) costs incurred as a result of the event, including expenses directly linked to the event (such as legal expenses and fees paid to advisors or suppliers) and costs of repairs or replacements;

(c) provisions or reserves accounted for in the profit and loss accounts against the loss;

(d) losses temporarily booked in transitory or suspense accounts and not yet reflected in the profit and loss accounts;

(e) negative economic effects, booked in an accounting period, resulting from operational risk events affecting cash flows or financial statements in previous accounting periods.

(2) A ***recovery*** for an operational risk event is an independent occurrence, related to the event, but separate in time, in which funds, or inflows of economic benefits, are received from a third party.

Examples

payments received from takaful entities

repayments received from perpetrators of fraud

recoveries of misdirected transfers

(3) The ***net loss*** for an operational risk event is the loss resulting from the event after any recovery.

7.3.3 Reporting to Regulatory Authority

The Regulatory Authority may, by notice given to an Islamic banking business firm, require the firm to report internal loss data in the level 1 categories set out in Annex 9, *Detailed loss event classification*, to *International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version*, published by the Basel Committee on Banking Supervision in June 2006.

Part 7.4 Operational risk capital requirement

Division 7.4.A Basic indicator approach

7.4.1 Sunset provision—Division 7.4.A

This Division ceases to have effect immediately before Division 7.4.B commences.

Note Division 7.4.B commences on 1 January 2023—see rule 7.4.3.

7.4.2 Basic indicator approach—calculation

(1) An Islamic banking business firm must use the basic indicator approach to operational risk. ***Operational risk capital requirement*** is the amount of capital that the firm must have to cover its operational risk.

(2) The firm's operational risk capital requirement is calculated in accordance with the following formula:

$$\frac{GI \times \alpha}{n}$$

where:

GI is the firm's average annual gross income (as defined in subrule (3) or (4)) for those years (out of the previous 3 years) for which the firm's annual gross income is more than zero.

α is 15% or a higher percentage set by the Regulatory Authority.

n is the number of years out of the previous 3 years for which the firm's gross income is more than zero.

Guidance

Because of the definitions of ***GI*** and ***n,*** figures for any year in which the annual gross income of a firm is negative or zero must be excluded from both the numerator and denominator when calculating the average.

(3) ***Gross income***, for a year, means the total of the following income for the year:

(a) net income from financing activities, which is gross of provisions, operating expenses and depreciation of *ijarah* assets;

(b) net income from investment activities, which includes the firm's share of profit from *mudarabah* and *musharakah*;

(c) fee income, which includes commissions and agency fees;

less the firm's share in income attributable to IAHs and other account holders.

(4) ***Gross income*** excludes:

(a) realised profits from the sale of securities in the banking book;

(b) realised profits from securities in the 'Held to Maturity' category in the banking book;

(c) extraordinary or irregular items of income;

(d) income derived from takaful;

(e) any collection from previously written-off loans; and

(f) income obtained from the disposal of real estate and other assets during the year.

Division 7.4.B Standardised approach

7.4.3 Commencement—Division 7.4.B

This Division commences on 1 January 2023.

7.4.4 Standardised approach—calculation

(1) An Islamic banking business firm must use the standardised approach to operational risk. ***Operational risk capital requirement*** is the amount of capital that the firm must have to cover its operational risk.

(2) The standardised approach is based on the following factors:

(a) the ***business indicator*** (***BI***), which is a financial-statement-based proxy for operational risk;

(b) the ***business indicator component*** (***BIC***), which is calculated by multiplying the BI by a set of marginal coefficients;

(c) the ***internal loss multiplier*** (***ILM***), which is a scaling factor that is based on a firm's average historical losses and the BIC.

(3) The business indicator is the sum of:

(a) the ***profit, ijarah instalments and dividend component*** (***PIDC***);

(b) the ***services component*** (***SC***): and

(c) the ***financial component*** (***FC***);

where ***PIDC***, ***SC*** and ***FC*** are calculated as set out in rule 7.4.5.

7.4.5 Calculation of *PIDC*, *SC* and *FC*

(1) In a formula in this rule, a bar above a term means that the term is to be calculated as the average of the relevant quantity over the current accounting year and the 2 previous accounting years of the firm concerned.

(2) The factors PIDC, SC and FC are calculated in accordance with the following formulas:

$$PIDC = Min\,[\overline{Abs\,(profit\ earned - expenses\ paid)};\ 2.25\%\ \overline{profit\ earning\ assets}] + \overline{dividend\ income}$$

$$SC = Max\left[\overline{Other\ operating\ income}; \overline{other\ operating\ expense}\right] + Max\,[\overline{Fee\ income}; \overline{fee\ expense}]$$

$$FC = \overline{Abs(net\ P\&L\ trading\ book)} + \overline{Abs(net\ P\&L\ banking\ book)}.$$

Guidance—meaning of business indicator terms

P&L or balance-sheet items	Description	Typical sub-items
Profit, *ijarah* rental and dividend component		
Profit income	Profit income from all financings, financial assets and other profit income (includes profit income from *ijarah* contracts)	• Profit income from all financings, assets available for sale, assets held to maturity, trading assets, ijarah rentals • Profit income from Shari'a-compliant hedge accounting • Other profit income, not included in the categories above • Profits from leased assets
Profit payment to fund providers	Profit payments on all financial liabilities and other return payments (includes rentals payable on ijarah losses, depreciation and impairment of ijarah assets)	• expenses or returns payable on funds received from investment account holders, current account deposits, debt securities issued, *ijarah* contracts
Profit-earning assets (balance sheet item)	Total gross outstanding financings, sukuk, other profit-bearing financial assets (including sovereign sukuk), and Ijarah assets measured at the end of each financial year	
Dividend income	Dividend income from investments in stocks and funds not consolidated in the firm's financial statements, including dividend income from non-consolidated subsidiaries, associates and joint ventures	
Services component		
Fee and commission income	Income received from providing advice and services. Includes income received by the firm as an outsourcer of financial services	Fee and commission income from: • securities (issuance, origination, reception, transmission, execution of orders on behalf of customers) • clearing and settlement; asset management; custody; fiduciary transactions; payment services; structured finance; servicing of securitisations; loan commitments and guarantees given

P&L or balance-sheet items	Description	Typical sub-items
Fee and commission expenses	Expenses paid for receiving advice and services. Includes outsourcing fees paid by the firm for the supply of financial services, but not outsourcing fees paid for the supply of non-financial services (for example, logistical, IT, human resources)	Fee and commission expenses from: • clearing and settlement; custody; servicing of securitisations; financing commitments and guarantees received; and foreign transactions
Other operating income	Income from ordinary banking operations not included in other BI items but of similar nature (income from operating *ijarah* transactions should be excluded)	• rental income from investment properties • gains from non-current assets and disposal groups classified as held for sale not qualifying as discontinued operations (IFRS 5.37)
Other operating expenses	Expenses and losses from ordinary banking operations not included in other BI items but of similar nature and from operational loss events (expenses from operating leases should be excluded)	• losses from non-current assets and disposal groups classified as held for sale not qualifying as discontinued operations (IFRS 5.37) • losses incurred as a consequence of operational loss events (for example fines, penalties, settlements, replacement cost of damaged assets), which have not been provisioned/reserved for in previous years • expenses related to establishing provisions/ reserves for operational loss events
Financial component		
Net profit (loss) on the trading book	• net profit/loss on trading assets and trading liabilities (*sukuk* securities, equity securities, financings, other assets and liabilities) • net profit/loss from hedge accounting • net profit/loss from exchange differences	

P&L or balance-sheet items	Description	Typical sub-items
Net profit (loss) on the banking book	• net profit/loss on financial assets and liabilities measured at fair value through profit and loss • realised gains/losses on financial assets and liabilities not measured at fair value through profit and loss (financing exposures, assets available for sale, assets held to maturity, financial liabilities measured at amortised cost) • net profit/loss from hedge accounting • net profit/loss from exchange differences	

7.4.6 Calculation of business indicator component

To calculate an Islamic banking business firm's BIC, the firm's BI is to be multiplied by 1 or more marginal coefficients. The firm's BIC is the sum of the amounts calculated by multiplying:

(a) the part of the firm's BI up to and including QR 5 billion by 12%;

(b) any part of the BI over QR 5 billion but not over QR 150 billion by 15%; and

(c) any part of the BI over QR 150 billion by 18%.

Guidance

The marginal coefficients increase with the size of the BI. For firms with a BI less than or equal to QR 5 bn, the BIC is equal to BI × 12%. For a BI of QR 165 bn, the BIC would be (5 x 12%) + (150 - 5) x 15% + (165 - 150) x 18% = QR 26.85 bn.

7.4.7 Calculation of internal loss multiplier

(1) An Islamic banking business form's ***internal loss multiplier*** (***ILM***) is intended to take into account the firm's operational risk experience in calculating the firm's operational risk capital requirement.

(2) The firm's ILM is calculated by the formula:

$$ILM = \ln\left(\exp(1) - 1 + \left(\frac{LC}{BIC}\right)^{0.8}\right)$$

where ***LC*** (the ***loss component***) is equal to 15 times the firm's average annual losses incurred over the previous 10 years as a result of operational risk events.

Guidance

The ILM is equal to 1 if the firm's loss component and business indicator component are equal. If the LC is greater than the BIC, the ILM is greater than 1. That is, a firm with losses that are high relative to its BIC is required to hold more capital. Conversely, if the LC is lower than the BIC, the ILM is less than 1 and the firm is required to hold less capital.

(3) If the firm holds 10 years of high-quality annual loss data, collected as set out in Part 7.3, the calculation of average losses for subrule (2) must be based on that 10 years of data. If the firm does not have 10 years of high-quality annual loss data, but has 5 years of such data, it may use the 5 years of data.

7.4.8 Calculation of operational risk capital requirement

(1) An Islamic banking business firm's operational risk capital requirement is the product of the firm's BIC and its ILM.

(2) However:

(a) if an Islamic banking business firm's loss data does not meet the standards set out in Part 7.3 for the whole of the previous 5-year period, the firm's operational risk capital requirement is equal to its BIC; and

(b) the Regulatory Authority may direct the firm to apply an ILM greater than 1.

7.4.9 Approval of exclusion of certain losses from dataset

The Regulatory Authority may approve the exclusion, by an Islamic banking business firm, of an operational loss event, or a class of operational loss events, from the firm's operational loss dataset if the Authority is satisfied that the event, or events of that class, are no longer relevant to the firm's risk profile.

Guidance

Approval to exclude internal loss events will be granted rarely and an application to do so must be supported by strong justification. In evaluating the relevance of an operational loss event to the firm's risk profile, the Authority will consider whether the cause of the event could occur in other areas of the firm's operations. Taking settled legal exposures and divested activities as examples, the Authority will expect the firm to demonstrate that there is no similar or residual legal exposure and that the event to be excluded has no relevance to other continuing activities or products.

The Authority will approve such an exclusion only if satisfied that the loss to be excluded is material to the firm's operations (for example, that the relevant loss is greater than 5% of the firm's average losses).

The Authority will approve the exclusion of a loss event (except for losses related to divested activities) only after it has been included in the firm's operational loss dataset for a minimum period (for example, 3 years).

Division 7.4.C Additional powers of Regulatory Authority

7.4.10 Powers of Regulatory Authority in relation to operational risk capital requirement

Despite anything in Division 7.4.A or 7.4.B, if the Regulatory Authority identifies points of exposure or vulnerability to operational risk that are common to 2 or more Islamic banking business firms, it may impose specific capital requirements or limits on each affected firm.

Examples

- outsourcing of important operations by many Islamic banking business firms to a single provider
- severe disruption to providers of payment and settlement services.

Part 7.5 Guidance on operational risks relating to Islamic financial contracts

7.5.1 Introduction

(1) This Part gives guidance on the Shari'a requirements in relation to Islamic financial contracts and on the operational risks that may arise from them.

(2) An Islamic banking business firm's failure to comply with the requirements, or any lack of precision in contract documentation, can give rise to Shari'a non-compliance risk.

Note The section is taken from IFSB-15: Revised Capital Adequacy Standard for Institutions Offering Islamic Financial Services, but the requirements may vary depending of the views of different Shari'a supervisory boards. 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.

7.5.2 Requirements for *murabahah* and *ijarah* contracts

(1) The asset is in existence at the time of sale or lease or, in the case of *ijarah*, the lease contract is preceded by acquisition of the usufruct of that asset (except if the asset was agreed upon based on a general specification).

(2) The asset is in the legal and constructive possession of the Islamic banking business firm when it is offered for sale or lease.

(3) The asset is intended to be used by the buyer or lessee for activities or businesses permissible by Shari'a. If the asset is leased back to its owner in the first lease period, it does not lead to a contract of *'inah.*

Note An ***'inah*** (also called *bay 'inah* or *bay-al inah*) is a double sale by which the borrower and the lender sell and then resell an asset between them, once for cash and once for a higher price whose payment is deferred. The net result is a loan with interest and, as such, is prohibited by the majority of Shari'a scholars.

(4) There is no late payment penalty fee or increase in price in exchange for extending or rescheduling the date of payment of accounts receivable or lease receivable, irrespective of whether the obligor is solvent or insolvent.

7.5.3 Requirements for *salam* and *istisna* contracts

(1) Sale and purchase contracts cannot be interdependent and interconditional on each other (such as *salam* and parallel *salam*, or *istisna* and parallel *istisna*).

(2) The is no penalty clause for delay in the delivery of a commodity that is purchased under a *salam* contract. However, such a penalty clause is allowed under *istisna* and parallel *istisna*.

Note An essential characteristic of a *salam* or *istisna* contract is that the subject matter does not, and is not required to, exist physically when the parties enter into the contract.

7.5.4 Requirements for *mudarabah* and *musharakah* contracts

(1) The capital of the Islamic banking business firm should be invested in Shari'a-compliant investments or business activities.

(2) A partner in *musharakah* cannot guarantee the capital of another partner, nor may the *mudarib* guarantee the capital of the *mudarabah*.

(3) The purchase price of another partner's share in a *musharakah* with a binding promise to purchase can only be set at market value or according to an agreement entered into at the time the contract became binding. However, the agreement should not stipulate that the share be purchased at its nominal value based on the capital originally contributed.

7.5.5 Operational risks—*murabahah*

(1) At the time the *murabahah* contract becomes binding, it is required that an Islamic banking business firm has purchased the asset and had it in its legal or constructive possession before selling it to the customer. Therefore, the firm should ensure that the legal characteristics of the contract properly match the commercial intent of the transactions.

(2) If the *mudarabah* customer acts as the agent of the firm for purchasing the asset, title to the asset should first pass to the firm and not directly to the customer.

7.5.6 Operational risks—*salam*

(1) This section sets out some of the operational risks that may arise when an Islamic banking business firm purchases from a customer, under a *salam* contract, goods against advanced payment.

(2) If the underlying goods delivered are of an inferior quality to that specified in the contract, the Islamic banking business firm (as buyer) should:

(a) reject the goods; or

(b) accept them at the originally agreed price.

In the latter case, the firm may suffer loss if it sells the goods at a lower price than would have been obtained for those specified in the contract.

Note In case of a parallel *salam*, however, the buyer of the commodity from the Islamic banking business firm may (but is not obliged to) agree to accept the goods at the contract price. In such a case, the firm does not suffer any loss of profit.

(3) The underlying goods may be delivered by the customer before the agreed date. If the goods delivered meet the contract specifications, the Islamic banking business firm (as buyer):

(a) normally has to accept the goods before the agreed delivery date; and

(b) may incur additional costs for storage, *takaful* cover and deterioration (if the goods are perishable) before the goods are resold.

(4) The *salam* contract may include a provision for restitution to be made to the firm for any loss suffered under subsection (2) or costs incurred under subsection (3).

(5) The firm may face legal risk if the goods in a parallel *salam* cannot be delivered to the parallel *salam* buyer because of:

(a) late delivery by the *salam* seller (the customer); or

(b) delay by the firm itself.

For legal risk not to arise in such a case, the parallel *salam* buyer will have to agree to change the delivery date of the goods.

7.5.7 Operational risks—*istisna*

(1) In the case of *istisna* with parallel *istisna*, an Islamic banking business firm contracts to deliver a constructed or manufactured asset and

enters into a contract with a subcontractor to construct or manufacture the asset.

(2) The reliance of the firm on the subcontractor can expose it to various operational risks such as those set out in subsections (3) to (6). These risks need to be managed by a combination of:

(a) legal precautions;

(b) due diligence in choosing subcontractors; and

(c) selection of suitably qualified consultants and staff to carry out the contract with the subcontractor and, ultimately, deliver the constructed or manufactured asset to the customer.

(3) In case of late delivery by the subcontractor, the firm may be unable to deliver the asset to the ultimate counterparty on the agreed date, and can, therefore, be subject to penalties for late delivery.

(4) In case of cost overruns during the construction or manufacturing process (because of increases in the prices of raw materials, increases in manufacturing or production costs or delays by the subcontractor), additional costs may have to be absorbed wholly or partly by the firm, in the absence of an agreement in advance with the ultimate counterparty.

(5) If the subcontractor fails to meet quality standards or other specifications agreed with the ultimate counterparty, the firm may face legal risk if no agreement is reached with the subcontractor and the ultimate counterparty:

(a) for remedying the defects; or

(b) for reducing the contract price.

(6) If the subcontractor fails to complete the asset on time, the firm may have to find a replacement from the market and can, therefore, be subject to additional costs.

7.5.8 Operational risks—*ijarah* and IMB contracts

(1) In an *ijarah* or IMB contract, an Islamic banking business firm (as lessor) may face, during the period of lease, the operational risks set out in this section.

(2) The ultimate use of the *ijarah* asset should be Shari'a-compliant. Otherwise, the firm will be exposed to non-recognition of the *ijarah* income as non-permissible, and the firm will be required to repossess the asset and find a new lessee.

(3) If the lessee damages the asset in its possession and refuses to pay for the damage, the firm will have to repossess the asset and take legal action to cover damages. This might involve operational and litigation costs.

(4) If the asset is severely damaged or destroyed without the fault of the lessee, the firm (as lessor) is required to provide a replacement to the lessee. If the asset is not insured, the firm will have to bear the cost of buying the new asset.

(5) Further, if the firm fails to provide the lessee with a replacement, the lessee may terminate the *ijarah* contract without paying the rentals for the remaining period.

(6) If the asset is damaged without the fault of the lessee, but can still be used, the firm (as lessor) is required to decrease the amount of the rentals. The decrease should be proportionate to the decrease in the utility of the asset.

(7) In the event of default or misconduct by the lessee, the firm may face legal risk in relation to the enforcement of its contractual right to repossess the asset.

7.5.9 Operational risks—*musharakah*

(1) In a *musharakah* contract, an Islamic banking business firm provides financing on the basis of a profit-sharing and loss-sharing contract.

(2) The firm may fail to carry out adequate due diligence on the customer or the financed venture.

(3) During the period of the investment, the firm may fail to monitor the venture's financial performance adequately or may not receive the required information from the customer.

7.5.10 Operational risks—*mudarabah*

(1) In a *mudarabah* contract, an Islamic banking business firm provides financing on the basis of a profit-sharing and loss-bearing contract.

(2) The firm's customer (as *mudarib*) is not required to bear any losses, in the absence of negligence, misconduct, fraud or breach of contract on its part. The customer is required to act in a fiduciary capacity as the manager of the firm's funds.

(3) The absence of the firm's right to control the management of the enterprise as capital provider (*rabb al-mal*) may give rise to operational risk.

(4) The customer may fail to provide the firm with regular, adequate and reliable information about the financial performance of the venture.

(5) The firm may fail to carry out adequate due diligence on the customer or the financed venture.

Explanatory note

This amendment substitutes a new Chapter 7 regarding operational risk and the calculation of an Islamic banking business firm's operational risk capital requirement.

[1.5] Glossary (definition of *CTRL*)

substitute

CTRL means the *Governance and Controlled Functions Rules 2020*.

Explanatory note

This amendment substitutes a definition.