OPERATIONAL RISK MANAGEMENT MODULE

MODULE	OM Operational Risk Management

Table of Contents

Table of Contents (continued)

OM-A.1 Purpose

Executive Summary

OM-A.1.1 The Operational Risk Management Module sets out the Central Bank of Bahrain's ('CBB's') rules and guidance to Islamic Bank licensees operating in Bahrain on establishing parameters and control procedures to monitor and mitigate operational risks. The contents of this Module apply to all Islamic banks, except where noted in individual Chapters.

OM-A.1.2 This Module provides support for certain other parts of the Rulebook, mainly:
(a) Principles of Business; ~~and~~
(b) High-level Controls;
(c) Reputational Risk;
(d) Internal Capital Adequacy Assessment Process ('ICAAP');
(e) Stress Testing; and
(f) Shari'a Governance.

Legal Basis

OM-A.1.3 **This Module contains the CBB's Directive (as amended from time to time) relating to Operational Risk Management and is issued under the powers available to the CBB under Article 38 of the Central Bank of Bahrain and Financial Institutions Law 2006 ('CBB Law'). The Directive in this Module is applicable to all Islamic bank licensees (including their approved persons).**

OM-A.1.4 For an explanation of the CBB's rule-making powers and different regulatory instruments, see Section UG-1.1.

OM-A.2 [This Chapter was deleted in October 2007]

OM-A.3 Module History

OM-A.3.1 This Module was first issued in July 2004 as part Volume one of the CBB Rulebook ~~(Volume one). All directives in this Module have been effective since this date. Any material~~ Material changes that have subsequently been made to this Module are annotated with the calendar quarter date in which the change was made; Chapter UG-3 provides further details on Rulebook maintenance and version control.

~~OM-A.3.2 When the CBB replaced the CBB in September 2006, the provisions of this Module remained in force. Volume 1 was updated in October 2007 to reflect the switch to the CBB; however, new calendar quarter dates were only issued where the update necessitated changes to actual requirements.~~ [This Paragraph was deleted in March 2019]

OM-A.3.3 The ~~most recent~~changes made to this Module are detailed in the table below:

Summary of Changes

Module Ref.	Change Date	Description of Changes
OM-5.1	01/04/05	Physical security measures.
OM-4.2	01/10/05	Succession planning for locally incorporated banks.
OM-5.1	01/10/05	Clarification of security manager role for smaller banks and deletion of requirement for cash trays.
OM-B & OM-1.2	01/04/06	Minor amendments concerning roles of Board and management and editing of OM B.
OM-5.1.15-OM-5.1.24	01/04/06	New security requirements for ATM security arrangements and reporting of security related complaints.
OM-A.2.1-OM-A.2.6	01/10/07	Purpose (expanded)
OM-A.2.1-OM-A.2.6	01/10/07	Key Requirements (deleted)
OM-5.1-OM-5.9	01/10/07	Business Continuity Planning (expanded)
OM-7	01/10/07	New Books and Records Chapter transferred from Module GR
OM-8	01/04/08	Basel II Qualitative Operational Risk Requirements
OM	01/2011	Various minor amendments to ensure consistency in CBB Rulebook.
OM-A.1.3 and OM-A.1.4	01/2011	Clarified legal basis.
OM-7.1.4	04/2011	This paragraph was deleted as Ministerial Order 23 does not apply to CBB licensees.
OM-7.3.4	04/2011	Clarified retention period of records for promotional schemes.
OM	07/2011	Various minor amendments to clarify Rules and have consistent language.
OM-2.4	07/2011	Amended CBB reporting requirements regarding succession planning.
OM-3.1.7	07/2011	Paragraph deleted as no longer applicable since standard conditions and licensing criteria document has now been incorporated as part of Volume 1.
OM-6.2	10/2011	Added new Section on internet security.
OM-7.1.7	10/2011	Corrected typo.
OM-A.1.3	01/2012	Updated legal basis.
OM-2.1.4	01/2012	Corrected cross reference.
OM-3.2.2	04/2012	Deleted last sentence of Paragraph as it repeats the requirement under Paragraph OM-3.3.1
OM-6.2.2	04/2012	Clarified penetration testing interval for internet security.
OM-1.1.4	10/2012	Amended to reflect updated version of Basel Committee document.
OM-3.2.6, OM-5.2.1, OM-5.4.8, OM-8	10/2012	Amended to reflect the Basel June 2011 paper on Principles for the Sound Management of Operational Risk.

OM-A.3 Module History (continued)

OM-A.3.3 (continued)

Summary of Changes

Module Ref.	Change Date	Description of Changes
OM-6.2	07/2013	Amended reporting requirements related to internet security measures.
OM-6.2.1	10/2013	Amended Rule to apply to all banks.
OM-3.7.2	10/2015	Clarified Rule on internal audit outsourcing.
OM-6	04/2016	Updated ATM security measures for banks.
OM-3.9	07/2016	Added new Section dealing with outsourcing of functions containing customer information.
OM-5.10	10/2016	Added new Section on Cyber Security Risk Management
OM-6.1.1	10/2016	Added implementation deadline date
OM-6.4.3	10/2016	Corrected cross references
OM-6.4.4	10/2016	Corrected cross references
OM-6.4.5	10/2016	Corrected cross references
OM-6.6	10/2016	Added new Section on Cyber Security Measures
OM-3.9.2	01/2017	Amended Paragraph on customer information
OM-3.9.6	01/2017	Added new guidance paragraph on customer information
OM-6.4.22	04/2017	ATM requirement on Solid Wall deleted.
OM-6.4.23	04/2017	ATM requirement on Solid Wall deleted.
OM-6.3.1	07/2017	Clarified requirements on compliance date.
OM-6.3.2A	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-6.3.2B	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-6.3.2C	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-6.3.2D	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-6.3.2E	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-6.4.21	07/2017	Deleted paragraph.
OM-7.2.1	07/2017	Amended paragraph according to the Legislative Decree No. (28) of 2002.
OM-7.2.2	07/2017	Deleted paragraph.
OM-3.1.2	10/2017	Amended paragraph to allow the utilization of cloud services.
OM-3.1.5A	10/2017	Added a new paragraph on outsourcing requirements.
OM-3.2.3	10/2017	Amended paragraph.
OM-3.3.1	10/2017	Amended paragraph.
OM-3.3.2	10/2017	Amended paragraph.
OM-3.3.3	10/2017	Amended paragraph.
OM-3.3.4	10/2017	Amended paragraph.
OM-3.3.5	10/2017	Added a new paragraph on outsourcing.
OM-3.4.1	10/2017	Amended paragraph.
OM-3.4.2(b)	10/2017	Amended sub-paragraph.
OM-3.4.3	10/2017	Deleted paragraph.
OM-3.4.5	10/2017	Amended paragraph.
OM-3.5.1(a)	10/2017	Amended sub-sub-paragraph no. (5).
OM-3.5.1(c)	10/2017	Amended sub-sub-paragraphs no. (2) and (3).
OM-3.5.1(e)	10/2017	Amended sub-sub-paragraph no. (3).
OM-3.8.3	10/2017	Amended paragraph.
OM-3.9.1	10/2017	Amended paragraph.
OM-3.9.2	10/2017	Amended paragraph on third party outsourcing of functions.
OM-3.9.3	10/2017	Amended paragraph.
OM-3.9.4)	10/2017	Amended paragraph.
OM-3.9.4(b)	10/2017	Amended sub-paragraph.
OM-3.9.4(d)	10/2017	Deleted sub-paragraph.
OM-3.9.5	10/2017	Deleted paragraph.
OM-3.9.7	10/2017	Added a new paragraph for security measures related to cloud services.
OM-6.4.6	10/2017	Amended paragraph to include ancillary service providers.

OM-A.3 Module History (continued)

OM-A.3.3 (continued)

Summary of Changes

Module Ref.	Change Date	Description of Changes
OM-6.3.1A	04/2018	Added a new Paragraph on card (EMV) compliance.
OM-6.3.1B	04/2018	Added a new Paragraph on "provision of cash withdrawal and payment services through various channels".
OM-6.3.2	04/2018	Amended Paragraph to mention "Islamic bank licensees".
OM-3.9.2	07/2018	Amended Paragraph to include call centres.
OM-3.9.2A	07/2018	Added new Paragraph on customer notification.
OM-6.4.15A	10/2018	Added a new Paragraph on drive-thru ATMs.
OM-6.4.20A	10/2018	Added a new Paragraph on drive-thru ATMs.
Various	03/2019	Various changes for better alignment with the principles and guidance from Basel Committee on Banking Supervision
OM-6.6	03/2019	Amended Section OM-6.6 to enhance cyber security measures

Evolution of the Module

OM-A.3.4 [Deleted in October 2007 updates]

OM-B.1 This Section was moved to Chapter OM-1.

OM-1.1 [This Chapter was deleted in March 2019]

~~Guidance Provided by International Bodies~~

~~Guidance Provided by other International Bodies~~

~~OM-1.1.1 The papers below provide guidance which promotes best practice and can be generally applied by all licensees to their activities.~~

~~Basel Committee: Framework for Internal Controls Systems in Banking Organisations~~

~~OM-1.1.2 The paper (see www.bis.org/publ/bcbs40.pdf) issued in September 1998 presents the first internationally accepted framework for supervisors to use in evaluating the effectiveness of the internal controls over all on- and off-balance sheet activities of banking organisations.~~

~~OM-1.1.3 The paper describes elements that are essential to a sound internal control system, recommends principles that supervisors can apply in evaluating such systems, and discusses the role of bank supervisors and external auditors in this assessment process.~~

~~Basel Committee: Principles for the Sound Management of Operational Risk~~

~~OM-1.1.4 The paper (see www.bis.org/publ/bcbs195.pdf) issued in June 2011 by the Basel Committee on Banking Supervision, outlines a set of principles that provide a framework for the effective management and supervision of operational risk, for use by banks and supervisory authorities when evaluating operational risk management policies and practices.~~

~~OM-1.1.5 The paper also recognises that clear strategies and oversight by the Board of Directors and senior management, a strong operational risk culture and internal control culture (including, among other things, clear lines of responsibility and segregation of duties), effective internal reporting, and contingency planning are all crucial elements of an effective operational risk management framework for banks of any size and scope.~~

MODULE	OM: Operational Risk Management
CHAPTER	OM-1 International Guidance and Best Practice

OM-1.1 Guidance Provided by International Bodies (continued)

Basel Committee: Risk Management for Electronic Banking and Electronic Money Activities

OM-1.1.6 The paper (see www.bis.org/publ) issued in March 1998 provides guidelines for supervisory authorities and banking organisations as they develop methods for identifying, assessing, managing and controlling the risks associated with electronic banking and electronic money.

OM-1.1.7 The paper indicates that, while providing new opportunities for banks, electronic banking and electronic money activities carry risks as well as benefits and it is important that these risks are recognised and managed in a prudent manner.

Basel Committee: Risk Management Principles for Electronic Banking

OM-1.1.8 The paper (see www.bis.org/publ) issued in July 2003 recognizes new risks associated with the increase in distribution of financial services through electronic channels, or e-banking. To emphasize the importance of these risks, the Committee has placed responsibility on the shoulders of the Board and senior management to ensure their institutions have analysed, identified and modified operations to mitigate these risks.

OM-1.1.9 To facilitate these developments, the Committee has identified fourteen Risk Management Principles for Electronic Banking to help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities.

OM-1.1.10 The Risk Management Principles fall into three broad, and often overlapping, categories of issues that are grouped to provide clarity: Board and Management Oversight; Security Controls; and Legal and Reputational Risk Management.

Joint Forum: High Level Principles for Business Continuity

OM-1.1.11 This paper provides a broad framework for business continuity standards, and contains seven principles for regulators and industry participants to follow. It was published in August 2006 and is available in the "publications" section of the Basel Committee portion of the BIS website (www.bis.org).

OM-2.1 ~~Overview~~ Operational Risk Management Framework

Overview

OM-2.1.1 This Chapter provides guidance and rules ~~for~~ relating to operational risk and sets out the requirements for an appropriate risk management environment, including business continuity, outsourcing, ~~and~~ electronic banking, and cyber security. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events including internal and external frauds. This definition includes legal and Shari'a non-compliance risks, but excludes strategic and reputational risk. Legal risk is the risk arising from the potential that unenforceable contracts, lawsuits or adverse judgments may disrupt or otherwise negatively affect the operations or financial condition of a bank. As legal risk is one type of operational risk, banks should ensure that all regulations included in this Module are also applied to the management of legal risks requirement.

OM-2.1.2 Operational risk is inherent in all types of banks~~'~~ activities, and ~~therefore all new products and services should be reviewed for operational risks prior to their implementation. As these risks are important and~~ can result in substantial losses. ~~bank auditors should include operational audits in the scope of all audits.~~ Sound operational risk governance, therefore, relies upon three lines of defence:

(a) Business line management;
(b) An independent operational risk management unit; and
(c) Internal Audit and other independent review functions.

Additionally, all new products and services should be reviewed for operational risks prior to their implementation. A bank's internal auditors play an important role in controlling operational risks and should include operational audits in the scope of all audits.

~~OM-2.1.3 [This Paragraph was deleted in March 2019] The importance of operational risk has gained prominence as increasing reliance on sophisticated technology raises concerns of potential losses should unforeseen events cause technological failures. Banks have traditionally focused on controlling and mitigating credit and liquidity risks, however, enhanced levels of automation, while reducing costs and processing times, also pose potential risks. As such any one process or system failure may itself or through a series of systematic failures, cause financial or other losses to a bank. Therefore, it has become imperative that banks should establish policies and procedures to monitor and control operational risks.~~

~~OM-2.1.4 [This Paragraph was deleted in March 2019] The CBB will use the papers mentioned in Paragraphs OM-1.1.1 to OM-1.1.11 as guidelines in evaluation of the internal control systems of banks operating in Bahrain. Such evaluations will be made through the CBB's normal supervisory processes (e.g. meetings with management, on-site examinations (Module BR) and the use of appointed experts (Section BR-6.5)~~

OM-2.1 Operational Risk Management Framework (Continued)

OM-2.1.5 **It is important to consider Shari'a non-compliance risk as one of the main risks that banks must take into account as part of their enterprise-level risk evaluation. Banks must be aware of the implications of Shari'a non-compliance risk for the overall enterprise when Shari'a requirements and rulings are not effectively communicated, translated into internal policy, or observed by banks across different businesses and functional units.**

OM-2.1.6 Operational risk in Islamic banks are categorized into three main types: general risks, legal risks and Shari'a non-compliance risks. Shari'a non-compliance is a unique risk for Islamic banks resulting from non-compliance ~~of the bank~~ with the rules and principles of Shari'a~~in its products and services.~~ It is crucial to set up key risk indicators for identifying the Shari'a non-compliance risk inherent in different kinds of Shari'a-compliant contracts, and to outline a set of variables that help to estimate the likelihood and severity of Shari'a non-compliance risk. Refer to Appendix B for Shari'a requirements on financing contracts. ~~The CBB will use the papers mentioned in Paragraphs OM-1.1.1 to OM-1.1.11 as guidelines in evaluation of the internal control systems of banks operating in Bahrain. Such evaluations will be made through the CBB's normal supervisory processes (e.g. meetings with management, on-site examinations (Module BR) and the use of appointed experts (Section BR-6.5)~~

Board's role in Establishing a Strong Risk Culture

OM-2.1.7 **The Board of Directors must take the lead in establishing a strong operational risk management culture in the bank. The Board of Directors and senior management must establish a corporate culture that is guided by strong risk management, and that supports and provides appropriate standards and incentives for professional and responsible behaviour. ~~In this regard, it is the responsibility of the Board of Directors to ensure that a strong operational risk management culture exists throughout the whole organisation.~~**

OM-2.1.8 The actions of the Board and senior management, policy, procedures, processes and systems provide the foundation for a sound risk management culture. More details on the role of the Board and senior management are to be found in Chapters HC-1, HC-2, and HC-6. The Board should establish a code of conduct policy that sets clear expectations for integrity and ethical values of the highest standard, and identify acceptable business practices and prohibited conflicts (see Section HC-2.2). Banks should define enforcement measures that clearly assign responsibility to the designated unit within the bank to identify ~~the~~ any code of conduct incidence and take the corrective actions.

OM-2.1 Operational Risk Management Framework (Continued)

Operational Risk Management Framework

OM-2.1.9 **Banks must develop, implement and maintain an Operational Risk Management Framework (ORMF) that is fully integrated into the bank's overall risk management processes. The ORMF must consider a range of factors, including the nature, size, complexity and risk profile of the bank.**

OM-2.1.10 The Board of Directors and senior management should understand the nature and complexity of the risks inherent in the portfolio of bank 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.

OM-2.1.11 **A bank 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. The ORMF must be comprehensively and appropriately documented and must include definitions of operational risk and operational loss.**

OM-2.1.12 **At minimum, the ORMF documentation must clearly:**

(a) Identify the governance structures used to manage operational risk, including reporting lines and accountabilities;
(b) Identify Board approved policy and procedures;
(c) Describe the risk assessment tools and how they are used;
(d) Describe the bank's accepted operational risk appetite and tolerance (see Paragraphs OM-2.1.13 to OM-2.1.15), as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;
(e) Describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;
(f) Establish risk reporting and Management Information Systems ('MIS');
(g) Provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives;
(h) Provide for appropriate independent review and assessment of operational risk; and
(i) Specify the roles and responsibilities of line management for managing operational risk.

OM-2.1.13 **The Board of Directors must establish, approve and periodically review the ORMF. The Board of Directors must oversee senior management to ensure that the policy, procedures, processes and systems are implemented effectively at all decision levels.**

OM-2.1 Operational Risk Management Framework (Continued)

OM-2.1.14 **The Board of Directors shall:**

(a) Establish an operational risk strategy and supporting processes in line with evolving best practices to understand the nature and scope of the operational risk inherent in the bank's strategies and activities, and develop comprehensive, dynamic oversight and control environments that are fully integrated into, or coordinated with, the overall ORMF for managing all risks across the banks;

(b) Provide senior management with clear guidance and direction regarding the principles underlying the ORMF and approve the corresponding policy developed by senior management;

(c) Regularly review the ORMF to ensure that the bank has identified, and is managing the operational risk arising from, external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes or systems, including changes in risk profiles and priorities (e.g. changing business volumes); and

(d) Ensure that the bank's ORMF is subject to effective independent review by an external third party, other than the external auditor upon first implementation of the requirements in this Chapter, and subsequently, when there are material changes in the relevant Rulebook requirements or to the business conducted by the bank and/or its risk profile.

Risk appetite

OM-2.1.15 **The Board of Directors must approve and review the risk appetite and tolerance statement for operational risk that articulates the nature, the types and levels of operational risk that the bank is willing to assume.**

OM-2.1.16 When approving and reviewing the risk appetite and tolerance statement, the Board of Directors should consider all relevant risks, the bank's level of risk aversion, its current financial condition and the bank's strategic direction. The Board of Directors should approve appropriate thresholds or limits for specific operational risks.

OM-2.1.17 In addition to the review of material operational risks and limits, the Board should also consider changes in the external environment, material 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 or nature of limit breaches. The board should monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.

MODULE	OM: Operational Risk Management
CHAPTER	OM-2: General Requirements

OM-2.1 Operational Risk Management Framework (Continued)

Operations Risk Governance

OM-2.1.18 **Senior management must develop, for approval by the Board of Directors, a clear, effective and robust governance structure with well-defined, transparent and clear lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation, policy, procedures, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.**

OM-2.1.19 **Banks must have an Operational Risk Management Unit (ORMU), independent of the risk generating business lines and must be responsible for the design, maintenance and ongoing development of the ORMF within the bank. The ORMU must be adequately staffed with skilled resources.**

OM-2.1.20 Senior management is responsible for establishing and maintaining effective channels for internal review of operational risk issues, as well as ensuring adequate resolution processes. These should include systems to report, track and, when necessary, escalate issues to ensure resolution. Banks should be able to demonstrate that the three lines of defence (as highlighted in Paragraph OM-2.1.2) approach is operating satisfactorily and to explain how the Board and senior management ensure that this approach is implemented and operating in an appropriate and acceptable manner.

OM-2.1.21 **Senior management must translate the ORMF into specific processes and procedures that can be implemented and verified within the different business units. Senior management must clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability, and ensure that the necessary resources are available to manage operational risk in-line with the bank's risk appetite and tolerance statement. Furthermore, senior management must ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.**

OM-2.1.22 Senior management shall ensure that staff responsible for managing operational risk, coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services, such as insurance risk transfer and outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

OM-2.1 Operational Risk Management Framework (Continued)

OM-2.1.23 **The Head of the Operational Risk Management Unit must be of sufficient stature within the bank to perform his duties effectively, ideally evidenced by a title commensurate with other risk management units, such as Credit, Market and Liquidity Risk.**

OM-2.1.24 **Senior management must ensure that bank activities are conducted by staff with the necessary experience, qualifications, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the bank's risk policy must be independent from the units they oversee.**

OM-2.1.25 **Senior management must ensure that an appropriate level of operational risk training is available at all levels throughout the organisation. The training that is provided must reflect the seniority, role and responsibilities of the individuals for whom it is intended.**

OM-2.1.26 A bank's risk governance structure should be commensurate with the nature, size, operational complexity and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration:

(a) Committee structure;
(b) Committee composition; and
(c) Committee operation.

OM-2.1.27 Sound industry practice is for Operational Risk Committees (or the Risk Committee) to include a combination of members with expertise in business activities and financial, as well as risk managers.

OM-2.1.28 Committee meetings should be held at appropriate frequencies, with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

MODULE	OM: Operational Risk Management
CHAPTER	OM-2: General Requirements

OM-2.1 Operational Risk Management Framework (Continued)

Risk Identification and Assessment

OM-2.1.29 **Senior management must ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.**

OM-2.1.30 Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal factors (such as the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes and employee turnover) and external factors (such as changes in the broader environment and the industry and advances in technology). Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively. Banks should use the classification categories contained in Appendix A for determining and classifying operational risk events.

OM-2.1.31 Examples of tools that may be used for identifying and assessing operational risk include:

(a) Audit Findings: While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors;

(b) Internal Loss Data Collection and Analysis: Internal operational loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic. Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure;

(c) 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 organisations other than the bank. 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;

(e) Risk Assessments: In a risk assessment, often referred to as a Risk Self-Assessment ('RSA'), a bank 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-Assessments ('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 the RCSA output into metrics that give a relative ranking of the control environment;

OM-2.1 Operational Risk Management Framework (Continued)

(e) Business Process Mapping: Business process mappings identify the key steps in business processes, activities and organisational functions. They also 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. They also can help prioritise subsequent management action;

(f) Risk and Performance Indicators: Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank's risk exposure. Risk indicators, often referred to as Key Risk Indicators ('KRIs'), are used to monitor the main drivers of exposure associated with key risks. Performance indicators, often referred to as Key Performance Indicators ('KPIs'), 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;

(g) Scenario Analysis: Scenario analysis is a process of obtaining expert opinion of 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. Given the subjectivity of the scenario process, a robust governance ORMF is essential to ensure the integrity and consistency of the process;

(h) Measurement: Banks 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 of the model can be used in an economic capital process and can be allocated to business lines to link risk and return; and

(i) Comparative Analysis: Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank's operational risk profile. For example, comparison of the frequency and severity of internal data with RCSAs can help the bank 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 bank's exposure to potential risk events.

OM-2.1.32 **Banks must ensure that the internal pricing and performance measurement mechanisms appropriately take into account operational risk.**

MODULE	OM: Operational Risk Management
CHAPTER	OM-2: General Requirements

OM-2.1 Operational Risk Management Framework (Continued)

New Products, Process and Change Management

OM-2.1.33 **Senior management must establish an internal approval process for all new products, activities, procedures, processes and systems that fully assesses operational risk.**

OM-2.1.34 In general, a bank's operational risk exposure is increased when a bank engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Moreover, the level of risk may escalate when new products, activities, procedures, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business-critical operations.

OM-2.1.35 **A bank must have a policy and procedures that address the process for review and approval of new products, activities, procedures, processes and systems. The review and approval process must consider:**

(a) Inherent risks in the new product, service, or activity;
(b) Changes to the bank's operational risk profile and appetite and tolerance, including the risk of existing products, services 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, service or activity.

OM-2.1.36 **The approval process must also include ensuring that appropriate investment has been made for human resources and technology infrastructure before new products, services, activities or systems are introduced. The implementation of new products, activities, procedures, processes and systems must be monitored in order to identify any material differences to the expected operational risk profile, and to manage any unexpected risks.**

MODULE	OM: Operational Risk Management
CHAPTER	OM-2: General Requirements

OM-2.1 Operational Risk Management Framework (Continued)

OM-2.1.37 The use of technology-related products, activities, processes and delivery channels exposes a bank to strategic, operational and reputational risks, and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks. Sound technology risk management uses the same precepts as operational risk management and includes:

(a) Governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with, and supportive of, the bank's business objectives;
(b) Policy and procedures that facilitate identification and assessment of risk;
(c) Establishment of a risk appetite and tolerance statement, as well as performance expectations to assist in controlling and managing risk;
(d) Implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and
(e) Monitoring processes that test for compliance with policy thresholds or limits

Monitoring and Reporting

OM-2.1.38 Senior management must implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms must be in place at the board, senior management, and business line levels that support proactive management of operational risk.

OM-2.1.39 Banks must ensure that the operational risk reports are comprehensive, accurate, consistent and actionable across business lines and products.

OM-2.1.40 Reporting should be timely and a bank 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. The results of these monitoring activities must be included in regular management and Board reports, as must the assessments of ORMF performed by an external third party. Reports generated by (and/or for) supervisory authorities must also be reported internally to senior management and the Board, where appropriate.

OM-2.1.41 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. Operational risk reports should include:

(a) Breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits;
(b) Details of recent significant internal operational risk events and losses; and
(c) Relevant external events and any potential impact on the bank and operational risk capital.

MODULE	OM: Operational Risk Management
CHAPTER	OM-2: General Requirements

OM-2.1 Operational Risk Management Framework (Continued)

OM-2.1.42 Data capture and risk reporting processes should be analysed periodically with a view to continuously enhancing risk management performance, as well as advancing risk management policy, procedures and practices.

Controls and mitigation

OM-2.1.43 Banks must have a strong control environment that utilises policies, procedures, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

OM-2.1.44 Strong internal controls are a critical aspect of operational risk management, and the banks should establish clear lines of management responsibility and accountability for implementing a strong control environment. The control environment should provide appropriate independence/separation of duties between the operational risk management unit, business lines and support functions.

OM-2.1.45 An effective internal control environment also requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals, or a team without dual controls or other countermeasures may enable concealment of losses, errors or inappropriate actions. Therefore, areas of potential conflicts of interest must be identified, minimised, and subject to careful independent monitoring and review.

OM-2.1.46 In addition to segregation of duties and dual controls, banks should ensure that other traditional internal controls are in place, as appropriate, to address operational risk. Examples of these controls include:

(a) Clearly established authorities and/or processes for approval;
(b) Close monitoring of adherence to assigned risk limits or thresholds;
(c) Safeguards for access to, and use of, bank assets and records;
(d) Appropriate staffing level and training to maintain expertise;
(e) Ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;
(f) Regular verification and reconciliation of transactions and accounts; and
(g) A vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks

OM-2.1 Operational Risk Management Framework (Continued)

OM-2.1.47 Internal control consists of five interrelated components:

(a) Control environment: The Board of Directors and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal controls. All personnel at a banking organisation need to understand their role in the internal controls process and be fully engaged in the process;

(b) Risk assessment: An effective internal control system requires that the material risks that could adversely affect the achievement of the bank's goals are being recognised and continually assessed. This assessment should cover all risks facing the bank and the consolidated banking organisation (that is, credit risk, country and transfer risk, market risk, profit rate risk, liquidity risk, operational risk, legal risk and reputational risk). Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks;

(c) Control activities: Control activities should be an integral part of the daily activities of a bank. An effective internal control system requires that an appropriate control structure is set up, with control activities defined at every business level. These should include: Top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorisations; and a system of verification and reconciliation;

(d) Information and communication: An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision-making. Information should be reliable, timely, accessible, and provided in a consistent format. It requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements. It also requires effective channels of communication to ensure that all staff fully understand and adhere to policy and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel; and

(e) Monitoring activities: The overall effectiveness of the bank's internal controls should be monitored on an ongoing basis. Monitoring of key risks should be part of the daily activities of the bank, as well as periodic evaluations by the business lines and internal audit. There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately-trained and competent staff. The Internal Audit function, as part of the monitoring of the system of internal controls, should report directly to the Board of Directors or its Audit Committee, and to senior management. Internal control deficiencies, whether identified by business line, Internal Audit, or other control personnel, should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the Board of Directors.

OM-2.1 Operational Risk Management Framework (Continued)

OM-2.1.48 Control processes and procedures should be established and banks should have a system in place for ensuring compliance with a documented set of internal policies concerning the risk management system. Principal elements of this could include, for example:

(a) Top-level reviews of the bank's progress towards the stated objectives;
(b) Verifying compliance with management controls;
(c) Review of the treatment and resolution of instances of non-compliance;
(d) Evaluation of required approvals and authorisations to ensure accountability to an appropriate level of management; and
(e) Tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy.

OM-2.1.49 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 should be addressed through sound technology governance and infrastructure risk management programmes.

OM-2.1.50 Management must ensure the bank has a sound technology infrastructure that:

(a) Meets current and long-term business requirements by providing sufficient capacity for normal activity levels, as well as peaks during periods of market stress;
(b) Ensures data and system integrity, security, and availability; and
(c) Supports integrated and comprehensive risk management.

OM-2.1.51 Mergers and acquisitions resulting in fragmented and disconnected infrastructure, cost-cutting measures or inadequate investment can undermine a bank'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, or oversee and manage risk in periods of high growth. 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.

OM-2.1.52 In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party such as through insurance. The Board of directors should determine the maximum loss exposure the bank is willing, and has the financial capacity to assume, and should perform a regular review of the bank's risk and insurance management programme.

MODULE	OM: Operational Risk Management
CHAPTER	OM-2: General Requirements

OM-2.1 Operational Risk Management Framework (Continued)

OM-2.1.53 Because risk transfer is an imperfect substitute for sound controls and risk management programmes, banks should view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place 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 insurance truly reduce risk, transfer the risk to another business sector or area, or create a new risk (e.g. counterparty risk).

Public Disclosure

OM-2.1.54 A bank must have a formal disclosure policy approved by the Board of Directors that addresses the bank's approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, banks must implement a process for assessing the appropriateness of their disclosures, including the verification and frequency of them.

OM-2.1.55 A bank's public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations, and evolving industry practice. See also Chapter HC-8 and Chapter PD-1 on disclosure requirements.

OM-2.1.56 A bank should disclose its ORMF in a manner that will allow stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively.

OM-2.1.57 A bank's disclosures must be consistent with how senior management and the Board of Directors assess and manage the operational risk of the bank.

OM-2.1.58 A bank's public disclosures must allow stakeholders to assess its approach to operational risk management.

OM-2.1 Operational Risk Management Framework (Continued)

Independent Review

OM-2.1.59 **Bahraini *Islamic bank licensees* must ensure that the ORMF is subject to independent review by a third party consultant, other than the external auditor upon first implementation of the requirements in this Module, and subsequently, when there are material changes in the relevant Rulebook requirements or to the business conducted by the bank and/or its risk profile.**

OM-2.1.60 In the context of this Chapter, "independent review' has the following meaning:

(a) Verification of the ORMF performed by an external third party should cover the effectiveness of the overall ORMF, consistent with the policy approved by the Board of Directors, and also test validation processes to ensure that they are independent and implemented in a manner consistent with established bank policy;

(b) Validation ensures that the risk assessment and quantification systems used by the bank are sufficiently robust and provide assurance of the integrity of inputs, assumptions, processes and outputs. Specifically, the independent validation process should provide enhanced assurance that the risk management methodology results in an operational risk capital charge that credibly reflects the operational risk profile of the bank. In addition to the quantitative aspects of the validation, the validation of data inputs, methodology and outputs of operational risk models is important to the overall process; and

(c) One of the essential components of the validation exercise is the review of the stress testing results for operational risk. Refer to Module ST on stress testing for detailed guidance.

OM-2.1.61 **Resources involved in the independent third party review must be competent and appropriately trained. The independent third party must not have been previously involved in the development, implementation and operation of the ORMF. The independent review must verify that the ORMF has been implemented as intended and is functioning effectively. The independent reviewer must report on the overall appropriateness and adequacy of the ORMF and the associated governance processes across the bank.**

OM-2.2 [This Section was deleted in March 2019]~~Developing an Appropriate Risk Management Environment~~

~~OM-2.2.1 It must be standard practice for a bank's management to implement policies and procedures to manage risks arising out of a bank's activities. The bank must maintain written policies and procedures that identify the risk tolerances approved by the Board of Directors and must clearly delineate lines of authority and responsibility for managing the risks. Banks' employees and loan officers in particular must be fully aware of all policies and procedures that relate to their specific duties.~~

~~OM-2.2.2 The bank's strategy must define its tolerance for risk and lay out the Board's understanding of the specific characteristics of operational risk.~~

~~*The Board of Directors*~~

~~OM-2.2.3 The Board of Directors must be aware of the major aspects of the bank's operational risk as a distinct and controllable risk Category.~~

~~OM-2.2.4 The responsibilities of the Board of Directors of the bank must include:~~

~~(a) Approving the bank's operational risk strategy;~~
~~(b) Periodically reviewing the bank's operational risk strategy;~~
~~(c) Approving the basic structure of the framework for managing operational risk; and~~
~~(d) Ensuring that senior management is carrying out its risk management responsibilities.~~

OM-2.2 Developing an Appropriate Risk Management Environment (continued)

Senior Management

OM-2.2.5 The responsibilities of the senior management of the bank must include:

(a) Implementing the operational risk strategy approved by the Board of Directors;

(b) Ensuring that the strategy is implemented consistently throughout the whole banking organisation;

(c) Ensuring that all levels of staff understand their responsibilities with respect to operational risk management;

(d) Developing and implementing policies, processes and procedures for managing operational risk in all of the bank's products, activities, processes and systems;

(e) Developing succession plans for senior staff; and

(f) Developing Business Continuity Plans for the bank.

Management Information System

OM-2.2.6 The management information system of a banking organisation plays a key role in establishing and maintaining an effective operational risk management framework.

OM-2.2.7 *'Communication flow'* serves the purpose of establishing a consistent operational risk management culture across the bank. *'Reporting flow'* enables:

(a) Senior management to monitor the effectiveness of the risk management system for operational risk; and

(b) The Board of Directors to oversee senior management performance.

OM-2.3 [This Section was deleted in March 2019]~~Identification, Measurement, Monitoring and Control~~

~~OM-2.3.1 As part of an effective operational risk management system, banks must:~~

~~(a) Identify critical processes, resources and loss events;~~

~~(b) Establish processes necessary for measuring operational risk;~~

~~(c) Monitor operational risk exposures and loss events on an on-going basis; and~~

~~(d) Develop policies, processes and procedures to control or mitigate operational risk.~~

~~OM-2.3.2 Banks should assess the costs and benefits of alternative risk limitation and control strategies and should adjust their operational risk exposure using appropriate strategies, in light of their overall risk profile.~~

OM-2.4 Succession Planning

OM-2.4.1 Succession planning is an essential precautionary measure for a bank if its leadership stability – and hence ultimately its financial stability – is to be protected. Succession planning is especially critical for smaller institutions, where management teams tend to be smaller and possibly reliant on a few key individuals.

OM-2.4.2 **The CBB requires Bahraini Islamic bank licensees ~~locally incorporated banks~~ to document their Board-approved succession plans for their senior management team and have these ready at any time for onsite inspection by CBB staff.**

OM-2.4.3 **[This Paragraph was deleted in July 2011].**

OM-3.1 Introduction

OM-3.1.1 This Chapter sets out the CBB's approach to outsourcing by licensees. It also sets out various requirements that licensees must address when considering outsourcing an activity or function.

OM-3.1.2 **In the context of this Chapter, 'outsourcing' means an arrangement whereby a third party performs on behalf of a licensee an activity which was previously undertaken by the licensee itself (or in the case of a new activity, one which commonly would have been performed internally by the licensee). Examples of services that are typically outsourced include data processing, cloud services, customer call centres and back-office related activities.**

OM-3.1.3 Most of the Directives in this Chapter are concerned with situations where the third party provider is outside the licensee's group. Section OM-3.8, however, sets out the CBB's requirements when a service is outsourced to a company within the licensee's group.

OM-3.1.4 **The requirements in this Chapter only apply to 'material' outsourcing arrangements. These are arrangements that, if they failed in any way, would pose significant risks to the on-going operations of a licensee, its reputation and/or quality of service provided to its customers. For instance, the outsourcing of all or a substantial part of functions such as customer sales and relationship management, settlements and processing, IT and data processing, internal audit and financial control, would normally be considered 'material'.**

OM-3.1.4A Licensees should assess whether the function/activity/process being outsourced is material based on an assessment of various factors including but not limited to:

(i) The importance of the business activity to be outsourced in terms of its contribution to income and profit and the risk of potential loss should the outsourcing service provider fail to perform the service;

(ii) The impact on the licensee's reputation and brand value, and on its ability to achieve its business objectives, strategy and plans if there are disruptions, irregularities, frauds or other adverse events occurring with outsourcing service provider;

(iii) The impact on business continuity should the outsourcing service provider fail to perform the service.

OM-3.1 Introduction (continued)

(iv) The impact on the licensee's customers, should the outsourcing service provider fail to perform the service or encounter a breach of confidentiality or security;

(v) The cost of the outsourcing as a proportion of total operating costs of the licensee;

(vi) The degree of difficulty, including the time taken, in finding an alternative outsourcing service provider or bringing the business activity in-house;

(vii) The aggregate exposure to a particular outsourcing service provider in case where a licensee outsources various functions to the same outsourcing service provider;

(viii) The ability to maintain appropriate internal controls and meet regulatory requirements due to operational problems faced by the outsourcing service provider;

(ix) The affiliation or other relationship between the licensee and the outsourcing service provider; and

(x) Any other factor that the licensee may consider appropriate for evaluating the materiality of an outsourcing arrangement.

OM-3.1.5 Management should carefully consider whether a proposed outsourcing arrangement falls under this Chapter's definition of 'material'. If in doubt, management should consult with the CBB.

OM-3.1.5A **For outsourcing services that are not considered material outsourcing arrangements, licensees must submit a written notification to the CBB within 7 working days before committing to the new outsourcing arrangement.**

OM-3.1.6 **[This Paragraph was deleted in March 2019]** ~~**The requirements in this Chapter only apply to outsourcing arrangements entered into after May 2003. In the case of pre-existing outsourcing agreements, the CBB requires licensees to apply the requirements of this Chapter to the fullest extent possible when these arrangements are subsequently renewed.**~~

OM-3.1.7 **[This Paragraph was deleted in July 2011].**

MODULE	OM:	Operational Risk Management
CHAPTER	OM-3:	Outsourcing

OM-3.2 Supervisory Approach

OM-3.2.1 The CBB recognises the benefits that can potentially be achieved through outsourcing an activity to a third party provider. They can include reduced costs, enhanced service quality and a reduction in management time spent on non-core activities. However, outsourcing an activity also poses potential risks. These include the ability of the outsourcing service provider to maintain service quality levels, reduced control over the activity and access to relevant information, and increased legal and client confidentiality risks.

OM-3.2.2 The CBB's approach is to allow licensees the freedom to enter into outsourcing arrangements, providing these have been properly structured and associated risks addressed.

OM-3.2.3 ~~**The CBB expects licensees to have undertaken a thorough assessment of a proposal before formally submitting the request for prior approval to the CBB.** However,~~ The CBB ~~is also willing to~~ will discuss ideas informally at an early stage of development, on a 'no-commitment' basis. It especially encourages an early approach when the proposed outsourcing is particularly material or innovative.

OM-3.2.4 ~~**Once an outsourcing arrangement has been implemented, the CBB requires a licensee to continue to monitor the associated risks and the effectiveness of its mitigating controls. It will verify this through the course of its normal on-site and off-site supervisory processes, such as prudential meetings and on-site examinations.**~~ The CBB also requires access to the outsourcing service provider of the outsourced activity, which it may occasionally want to examine itself, through management meetings or on-site examinations.

OM-3.2.5 **Fundamental to the CBB's supervisory approach to outsourcing is that the Board and management of the licensee may not abdicate their responsibility for a licensee's business and the way its customers are treated. The Board and management remain ultimately responsible for the effectiveness of systems and controls in outsourced activities.**

OM-3.2 Supervisory Approach (continued)

OM-3.2.6 The board and senior management are responsible for understanding the operational and reputational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass:

(a) Procedures for determining whether and how activities can be outsourced;

(b) Processes for conducting due diligence in the selection of potential outsourcing service providers;

(c) Sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;

(d) Programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the outsourcing service provider;

(e) Establishment of an effective control environment at the bank and the service provider;

(f) Development of viable contingency plans; and

(g) Execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing service provider and the bank.

OM-3.3 Prior Approval Requests

OM-3.3.1 **A licensee must seek the CBB's prior written approval before committing to a new material outsourcing arrangement.**

OM-3.3.2 **The above request for prior approval must:**

(a) Be made in writing to the licensee's normal supervisory point of contact;

(b) Contain sufficient detail to demonstrate that relevant issues raised in ~~Section OM-3.4 onward of~~ this Chapter have been addressed; and

(c) Be made at least 6 weeks before the licensee intends to commit to the arrangement.

OM-3.3.3 The CBB will review the information provided and provide a definitive response within 6 weeks of receiving the request for prior approval. Where further information is requested from the licensee, however, the time taken to provide this further information will not be taken into account. The CBB may also contact home or host supervisors of the licensee or the outsourcing service provider, to seek their comments – in such cases, the 6-week turnaround is also subject to the speed of their response.

OM-3.3.4 **Once an activity has been outsourced, a licensee must immediately inform its normal supervisory point of contact at the CBB of any material problems encountered with the outsourcing service provider. The CBB reserves the right to direct a licensee to make alternative arrangements for the outsourced activity.**

OM-3.3.5 The CBB reserves the right to require a licensee to terminate or make alternative outsourcing arrangements if, among other reasons, the confidentiality of its customer information was, or is likely to be, breached or the ability of the CBB to carry out its supervisory functions in view of the outsourcing arrangement cannot be assured or executed.

OM-3.4 Risk Assessment

OM-3.4.1 Licensees must undertake a thorough risk assessment of an outsourcing proposal, before formally submitting the request for approval to the CBB and committing itself to an agreement.

OM-3.4.2 The risk assessment must – amongst other things – include an analysis of:

(a) The business case;

(b) The suitability of the outsourcing service provider; including but not limited to the outsourcing service provider's financial soundness, its technical competence, its commitment to the arrangement, its reputation, its adherence to international standards, and the associated country risk; and

(c) The impact of the outsourcing on the licensee's overall risk profile and its systems and controls framework.

OM-3.4.3 [This paragraph was deleted in October 2017].

OM-3.4.4 Once an outsourcing agreement has been entered into, licensees must:

(a) Regularly review the suitability of the outsourcing service provider and the on-going impact of the agreement on their risk profile and systems and controls framework. Such reviews must take place at least every year; and

(b) Monitor the associated risks and the effectiveness of its mitigating controls.

OM-3.4.5 A licensee must nominate a relevant approved person with day-to-day responsibility for handling the relationship with the outsourcing service provider and ensuring that relevant risks are addressed. This person must be notified to the CBB as part of the request for prior approval required under Section OM-3.3 above. Any subsequent replacement of such person must also be notified to the CBB.

OM-3.5 Outsourcing Agreement

OM-3.5.1 The activities to be outsourced and respective contractual liabilities and obligations of the outsourcing service provider and licensee must be clearly specified in an outsourcing agreement. This agreement must – amongst other things – address the following points:

(a) Control over outsourced activities

1. The Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in outsourced activities. Licensees must therefore ensure that they have adequate mechanisms for monitoring the performance of, and managing the relationship with, the outsourcing service provider;
2. A service level agreement ("SLA") – setting out the standards of service to be provided – must form part of the outsourcing agreement. Where the outsourcing provider interacts directly with a licensee's customers, the SLA must – where relevant – reflect the licensee's own standards and the CBB's relevant rulebook requirements regarding customer ~~care~~ service;
3. Mechanisms for the regular monitoring by licensees of performance against the SLA and other targets, and for implementing remedies in case of any shortfalls, must also form part of the agreement;
4. Clear reporting and escalation mechanisms must be specified in the agreement; and
5. Where an outsourcing service provider in turn decides to sub-contract to other providers, CBB's prior written approval must be obtained, and the original provider must remain contractually liable to the licensee for the quality and level of service agreed, and its obligations to the licensee must remain unchanged.

OM-3.5 Outsourcing Agreement (continued)

(b) Customer data confidentiality

1. Licensees must ensure that outsourcing agreements comply with all applicable legal requirements regarding customer confidentiality.
2. Licensees must ensure that the outsourcing service provider implements adequate safeguards and procedures. Amongst other things, customer data must be properly segregated from those belonging to other clients the outsourcing service provider may have. Outsourcing service providers must give suitable undertakings that the company and its staff will comply with all applicable confidentiality rules. Licensees must have contractual rights to take action against the service provider in the event of a breach of confidentiality.
3. Licensees must assess the impact of using an overseas-based outsourcing service provider on their ability to maintain customer data confidentiality, for instance, because of the powers of local authorities to access such data.

(c) Access to information

1. Outsourcing agreements must ensure that the licensee's internal and external auditors have timely access to any relevant information they may require to fulfill their responsibilities. Such access must allow them to conduct on-site examinations of the outsourcing service provider, if required.
2. Licensees must also ensure that the CBB inspectors and appointed experts have timely access to any relevant information they may reasonably require under the law. Such access must allow the CBB to conduct on-site examinations of the outsourcing service provider, if required.
3. Where the outsourcing service provider is based overseas, the outsourcing service provider must confirm in the outsourcing agreement that there are no regulatory or legal impediments to either the licensee's internal and external auditors, or the CBB inspectors and appointed experts, having the access described above. Should such restrictions subsequently be imposed, the licensee must communicate this fact to the CBB as soon as it becomes aware of the matter.

OM-3.5 Outsourcing Agreement (continued)

4. The outsourcing service provider must commit itself, in the outsourcing agreement, to inform~~ing~~ the licensee of any developments that may have a material impact on its ability to meet its obligations. These may include, for example, relevant control weaknesses identified by the outsourcing service provider's internal or external auditors, and material adverse developments in the financial performance of the outsourcing service provider.

(d) Business continuity

1. Licensees must ensure that service providers ~~maintain,~~ regularly review and test plans to ensure continuity in the provision of the outsourced service.
2. Licensees must have an adequate understanding of the outsourcing service provider's arrangements, to understand the implications for its own contingency arrangements (see Section OM-3.6).

(e) Termination

1. Licensees must have the right to terminate the agreement should the outsourcing service provider undergo a change of ownership (whether direct or indirect) that poses a potential conflict of interest; becomes insolvent; or goes into liquidation or administration.
2. Termination under any other circumstances allowed under the agreement must give licensees a sufficient notice period in which they can effect a smooth transfer of the service to another provider or bring it back in-house.
3. In the event of termination, for whatever reason, the agreement must provide for the return of all customer data – where required by licensees. ~~– or destruction of the records.~~

OM-3.6 Contingency Planning for Outsourcing Arrangements

OM-3.6.1 **Licensees must maintain and regularly review contingency plans to enable them to set up alternative arrangements – with minimum disruption to business – should the outsourcing contract be suddenly terminated or the outsourcing service provider fails. This may involve the identification of alternative outsourcing service providers or the provision of the service in-house. These plans must consider how long the transition would take and what interim arrangements would apply.**

OM-3.6.2 See Chapter OM-5 for further guidance on business continuity and contingency planning.

OM-3.7 [This Section was deleted in March 2019 and requirements were moved to Chapter HC-6.5] ~~Internal Audit Outsourcing~~

~~OM-3.7.1 Because of the critical importance of an effective internal audit function to a licensee's control framework, all proposals to outsource internal audit operations are to be considered material.~~

~~OM-3.7.2 The CBB will not permit licensees to outsource their internal audit function to the same firm that acts as their external auditor.~~

~~OM-3.7.3 Licensees who have existing outsourcing arrangements in place with their external auditor relating to the provision of internal audit services are required to find suitable alternatives when the existing arrangements terminate or come up for renewal.~~

~~OM-3.7.4 In all circumstances, Board and management of licensees must retain responsibility for ensuring that an adequate internal audit programme is implemented, and will be held accountable in this respect by the CBB.~~

OM-3.8 Intra-group Outsourcing

OM-3.8.1 **As with outsourcing to non-group companies, the Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in activities outsourced to group companies.**

OM-3.8.2 However, the degree of formality required – in terms of contractual agreements and control mechanisms – for outsourcing within a licensee's group is likely to be less, because of common management and enhanced knowledge of other group companies.

OM-3.8.3 **A licensee must seek the CBB's prior written approval at least 6 weeks before committing to a material intra-group outsourcing. The request for approval must be made in writing to the licensee's normal supervisory point of contact, and must set out a summary of the proposed outsourcing, its rationale, and an analysis of its associated risks and proposed mitigating controls. The CBB will respond to the request for approval in the same manner and timescale as set in Section OM-3.3 above.**

OM-3.8.4 **~~The CBB expects, a~~ As a minimum, an agreed statement of the standard of service ~~to~~ must be provided by the group provider, including a clear statement of responsibilities allocated between the group provider and licensee.**

OM-3.8.5 **~~The CBB also expects a~~ The licensee's management ~~to have~~ must address~~ed~~ the issues of customer confidentiality, access to information and business continuity covered above (Section OM-3.5).**

OM-3.9 Outsourcing of Functions Containing Customer Information

OM-3.9.1 Licensees must seek the CBB's prior written approval for third party and intragroup outsourcing of functions/services containing customer information including but not limited to payment services, debt collection, card and data processing, IT function including cloud services, internal audit and electronic/internet banking services but excluding legal services.

OM-3.9.1A Because of the critical importance of protecting customer information confidentiality, all proposals to outsource functions containing customer information should be considered material.

OM-3.9.2 For a third party outsourcing of functions/services containing customer information, other than debt collection, IT function, internal audit, cards embossing, cheques personalization, data/documents storing and call centres, the outsourcing service providers must be licensed by the CBB and located in Bahrain. If the outsourced service is not available in Bahrain after 30th June 2017, licensees must submit to the CBB a written request, at least within 30 days of the stated deadline. The request must provide details of the circumstances under which the extension of outsourcing activities is being requested.

OM-3.9.2A In case of an outsourcing arrangement that involves ~~transmission~~ disclosure of ~~customer~~ confidential information to the outsourcing service provider, Licensees must ~~make necessary changes to the terms of the customer agreements and send prior notices to the customer, who shall provide a consent in writing that his/her information would be transmitted to a service provider. Licensees may only effect the changes in the customer agreement following the receipt of customer consent.~~ ensure that the contract with the outsourcing service provider clearly requires the latter to safeguard the confidentiality of the confidential information; provided always that the responsibility for unlawful disclosure of such confidential information shall rest with the licensee. Due consideration must also be given to Law No. 30 of 2018, Personal Data Protection Law (PDPL) issued on 12 July 2018.

OM-3.9.3 ~~Licensees must provide to the CBB quarterly progress reports on the steps and procedures taken in implementing the requirements of Paragraph OM-3.9.2. The progress report must be provided to the retail bank's supervisory point of contact at the CBB and the first report must be submitted by 31st July 2016.~~
[This paragraph was deleted in March 2019]

MODULE	OM:	Operational Risk Management
CHAPTER	OM-3:	Outsourcing

OM-3.9 Outsourcing of Functions Containing Customer Information (continued)

OM-3.9.4 **For intra-group outsourcing of functions/services containing customer information, the following conditions must also be met:**

(a) The outsourcing service providers must be annually audited by the group internal audit team and the audit findings must be reported to the CBB;

(b) The service level agreement must clearly state that the CBB inspectors and appointed experts have the legal right to conduct onsite examinations of the outsourcing service provider and such expenses are to be borne by the retail bank;

(c) Any report by any other regulatory authority on the quality of controls of the outsourcing service provider must be submitted immediately by the licensee to the CBB; and

(d) [This sub-paragraph was deleted in October 2017].

OM-3.9.5 [This Paragraph was deleted in October 2017].

OM-3.9.6 In the case of overseas retail bank licensees, the CBB may consider a third party outsourcing arrangements entered by the licensee's head office as an intragroup outsourcing, provided that the head office submits to the CBB a letter of comfort which includes, but not limited to, the following conditions:

a. The head office declares its ultimate responsibility of ensuring that adequate controlling measures are in place; and
b. The head office is responsible to take adequate rectification measures, including compensation to the affected customers, in cases where customers suffer any loss due to inadequate controls applied by the third party service provider.

Cloud Services

OM-3.9.7 **For the purpose of outsourcing of cloud services, licensees must ensure that, at a minimum, the following security measures are in place:**

(a) Customer information must be encrypted and licensees must ensure that all encryption keys or similar forms of authentication are kept secure within the licensee's control;

(b) A secure audit trail must be maintained for all actions performed at the cloud services outsourcing service provider;

(c) A comprehensive change management procedure must be developed to account for future changes to technology with adequate testing of such changes;

OM-3.9 Outsourcing of Functions Containing Customer Information (continued)

(d) The licensee's data must be logically segregated from other entities data at the outsourcing service provider's platform;

(e) The cloud service provider must provide information on measures taken at its platform to ensure adequate information security, data security and confidentiality, including but not limited to forms of protection available against unauthorized access and incident management process in cases of data breach or data loss; and

(f) The right to release customer information/data in case of foreign government/court orders must be the sole responsibility of the licensee, subject to the CBB Law.

OM-4.1 Electronic Banking

OM-4.1.1 [This Paragraph was deleted in March 2019].~~This Chapter refers to Basel Committee papers that the CBB requires relevant licensees to use as guidance on electronic banking activities.~~

OM-4.1.2 **[This Paragraph was deleted in March 2019]. ~~The CBB considers that the following papers represent best practice and provide guidelines for recognising, addressing and managing risk associated with this area. Banks should take appropriate steps for the implementation of relevant recommendations set out therein:~~**

~~(a) 'Risk Management for Electronic Banking and Electronic Money Activities' issued in March 1998 (see OM-1.1 for further references to the paper);~~

~~(b) 'Risk Management Principles for Electronic Banking' issued in May 2001 (see OM-1.1 for further references to the paper).~~

OM-4.1.3 **[This Paragraph was deleted in March 2019]. ~~Licensees must use the 'Risk Management Principles and Sound Practices' in the Basel Committee paper in OM-1.1 as guidelines to recognise and prudently manage risks associated with e-banking.~~**

Board and Management Oversight

OM-4.1.4 **The Board of Directors and senior management must establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policy and controls to manage these risks.**

OM-4.1.5 **The Board of Directors and senior management must review and approve the key aspects of the licensee's security control process.**

OM-4.1.6 **The Board of Directors and senior management must establish a comprehensive and ongoing due diligence and oversight process for managing the licensee's outsourcing relationships and other third-party dependencies supporting e-banking.**

Security Controls

OM-4.1.7 **Licensees must take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business over the internet.**

OM-4.1 Electronic Banking (Continued)

OM-4.1.8	Licensees must use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions.
OM-4.1.9	Licensees must ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.
OM-4.1.10	Licensees must ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications.
OM-4.1.11	Licensees must ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.
OM-4.1.12	Licensees must ensure that clear audit trails exist for all e-banking transactions.
OM-4.1.13	Licensees must take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality must be commensurate with the sensitivity of the information being transmitted and/or stored in databases.
OM-4.1.14	Licensees must ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the licensee's identity and regulatory status of the licensee prior to entering into e-banking transactions.
OM-4.1.15	Licensees must take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the licensee is providing e-banking products and services.
OM-4.1.16	Licensees must have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.
OM-4.1.17	Licensees must develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks, that may hamper the provision of e-banking systems and services.

OM-5.1 Introduction

Why Do Financial Institutions Need Business Continuity Plans?

OM-5.1.1 All businesses may experience serious disruptions to their business operations. These disruptions may be caused by external events such as flooding, power failure or terrorism, or by internal factors such as human error or a serious computer breakdown. The probability of some events may be small, but the potential consequences may be massive, whereas other events may be more frequent and with shorter time horizons. ~~The Joint Forum (the Basel Committee on Banking Supervision (BCBS), the International Organisation of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS)) have given additional background and context to the need for business continuity in its paper of August 2006 titled "High Level Principles for Business Continuity" ().~~

OM-5.1.2 ~~According to the Joint Forum, in its paper, Business Continuity is "a whole of business approach for insuring that specified operations can be maintained or recovered in a timely fashion in the event of disruption. Its The~~ purpose of a Business Continuity Plan ('BCP') is to minimize the operational, financial, legal, reputational, and other material consequences arising from a disruption. The objectives of a good ~~business continuity plan ("BCP")~~ BCP are:

(a) To minimise financial loss to the licensee;

(b) To continue to serve customers and counterparties in the financial markets; and

(c) To mitigate the negative effects that disruptions can have on a licensee's reputation, operations, liquidity, credit quality, its market position, and its ability to remain in compliance with applicable laws and regulations.

OM-5.1.3 [This Paragraph was deleted in March 2019]. ~~Banks play a critical role in an economy, in providing payment services, as holders of people's savings, and as providers of finance. Hence, a BCP is especially critical for banks. It helps ensure that their business operations are resilient and the effects of disruptions in service are minimized and thus helps maintain confidence in the banking system.~~

OM-5.1 Introduction (continued)

Scope and Key Elements of a BCP

OM-5.1.4 **The requirements of this Chapter apply to all retail and wholesale banks (whether locally incorporated or a branch).**

OM-5.1.5 Branch Licensees of foreign banks may apply alternative arrangements to those specified in this module, where they are subject to comprehensive BCP arrangements implemented by their head office or other member of their group, provided that:

(a) They have notified the CBB in writing what alternative arrangements will apply;

(b) They have satisfied the CBB that these alternative arrangements are equivalent to the measures contained in this chapter, or are otherwise suitable; and

(c) The CBB has agreed in writing to these alternative arrangements being used.

~~***Implementation***~~

OM-5.1.6 **[This Paragraph was deleted in March 2019]** ~~**The requirements in this Chapter must be complied with in full by 1 October 2007. Failure to comply with these requirements after that will trigger a supervisory response, which may include formal enforcement measures, as set out in Module EN (Enforcement).**~~

OM-5.1.7 [This Paragraph was deleted in March 2019]. ~~For contingency planning relating to outsourcing activities, see Section OM-3.6.~~

OM-5.2 General Requirements

OM-5.2.1 **To ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption all Islamic bank licensees must maintain a business continuity plan (BCP) appropriate to the scale and complexity of their operations. A BCP must address the following key areas:**

(a) Data back up and recovery (hard copy and electronic);
(b) Continuation of all critical systems, activities, and counterparty impact;
(c) Financial and operational assessments;
(d) Alternate communication arrangements between the licensee and its customers and its employees;
(e) Alternate physical location of employees;
(f) Communications with and reporting to the CBB and any other relevant regulators; and
(g) Ensuring customers' prompt access to their funds in the event of a disruption.

OM-5.2.2 **Effective BCPs must be comprehensive, limited not just to disruption of business premises and information technology facilities, but covering all other critical areas, which affect the continuity of critical business operations or services (e.g. liquidity, human resources and others).**

OM-5.2.3 **Licensees must notify the CBB promptly if their BCP is activated. They must also provide regular progress reports – as agreed with the CBB – until the BCP is deactivated.**

OM-5.2.4 The CBB recognises that BCPs involve costs, and that it may not be cost effective to have a fully developed and implemented BCP for all conceivable worst-case scenarios. However, the CBB expects licensees to plan for how they may cope with the complete destruction of buildings and surrounding infrastructure in which their key offices, installations, counterparties or service providers are located. The loss of key personnel, and a situation where back-up facilities might need to be used for an extended period of time are important factors in effective BCPs.

OM-5.2.5 Licensees may find it useful to consider two-tier plans: one to deal with near-term problems; this should be fully developed and able to be put into immediate effect. The other, which might be in paper form; should deal with a longer-term scenario (e.g. how to accommodate processes that might not be critical immediately but would become so over time).

OM-5.3 Board and Senior Management Responsibilities

Establishment of a Policy, Processes & Responsibilities

OM-5.3.1 A ~~Bank's~~ Licensee's Board of Directors and Senior Management are collectively responsible for a bank's business continuity. The Board must endorse the policies, standards and processes for a licensee's BCP.~~as established by its senior management. The Board and senior management must delegate adequate resources to develop the BCP, and for its maintenance and periodic testing.~~

OM-5.3.2 Licensees must establish a Crisis Management Team (CMT) to develop, maintain and test their BCP, as well as to respond to and manage the various stages of a crisis. The CMT must comprise members of senior management and heads of major support functions (e.g. building facilities, IT, corporate communications and human resources).

OM-5.3.3 Licensees must establish (and document as part of the BCP) individuals' responsibilities in helping prepare for and manage a crisis; and the process by which a disaster is declared and the BCP initiated (and later terminated).

Monitoring and Reporting

OM-5.3.4 The CMT must submit regular reports to the Board and senior management on the results of the testing of the BCP (refer to section OM-5.9). Major changes must be developed by CMT, reported to senior management, and endorsed by the Board.

OM-5.3.5 The Chief Executive of a licensee must sign a formal annual statement submitted to the Board on whether the recovery strategies adopted are still valid and whether the documented BCP is properly tested and maintained. The annual statement must be included in the BCP documentation and will be reviewed as part of the CBB's on-site examinations.

OM-5.4 Developing a Business Continuity Plan

Impact Analysis

OM-5.4.1 **Licensees' BCPs must be based on (i) a business impact analysis (ii) an operational impact analysis, and (iii) a financial impact analysis. These analyses must be comprehensive, including all business functions and departments, not just IT or data processing.**

OM-5.4.2 The key objective of a Business Impact Analysis is to identify the different kinds of risk to business continuity and to quantify the operational and financial impact of disruptions on a licensee's ability to conduct its critical business processes.

OM-5.4.3 A typical business impact analysis is normally comprised of two stages. The first is to identify and prioritise the critical business processes that must be continued in the event of a disaster. The first stage should take account of the impact on customers and reputation, the legal implications and the financial cost associated with downtime. The second stage is a time-frame assessment. This aims to determine how quickly the licensee needs to resume critical business processes identified in stage one.

OM-5.4.4 Operational impact analysis focuses on the firm's ability to maintain communications with customers and to retrieve key activity records. It identifies the organizational implications associated with the loss of access, loss of utility, or loss of a facility. It highlights which functions may be interrupted by an outage, and the consequences to the public and customer of such interruptions.

OM-5.4.5 A Financial Impact Analysis identifies the financial losses that (both immediate and also consequent to the event) arise out of an operational disruption.

Risk Assessment

OM-5.4.6 **In developing a BCP, licensees must consider realistic threat scenarios that may (potentially) cause disruptions to their business processes.**

OM-5.4 Developing a Business Continuity Plan (continued)

OM-5.4.7 Licensees should analyse a threat by focusing on its impact on the business processes, rather than on the source of a threat. Certain scenarios can be viewed purely in terms of business disruption in specific work areas, systems or facilities. The scenarios should be sufficiently comprehensive to avoid the BCPs becoming too basic and thereby avoiding steps that could improve the resiliency of the licensee to disruptions.

OM-5.4.8 **Business continuity ~~plans~~ BCPs must take into account different types of likely or plausible scenarios to which the bank may be vulnerable. In particular, the following specific scenarios must at a minimum, be considered in the BCP:**

- **Utilities are not available (power, telecommunications);**
- **Critical buildings are not available or specific facilities are not accessible;**
- **Software and live data are not available or are corrupted;**
- **Vendor assistance or (outsourced) service providers are not available;**
- **Critical documents or records are not available;**
- **Critical personnel are not available; and**
- **Significant equipment malfunctions (hardware or telecom).**

OM-5.4.9 **Licensees must distinguish between threats with a higher probability of occurrence and a lower impact to the business process (e.g. brief power interruptions) to those with a lower probability and higher impact (e.g. a terrorist bomb).**

OM-5.4.10 **As a starting point, licensees must perform a "gap analysis". This gap analysis is a methodical comparison of what types of plans the licensee requires in order to maintain, resume or recover critical business operations or services in the event of a disruption, versus what the existing BCP provides. Management and the Board can address the areas that need development in the BCP, using the gap analysis.**

OM-5.5 BCP – Recovery Levels & Objectives

OM-5.5.1 **The BCP must document strategies and procedures to maintain, resume and recover critical business operations or services. The plan must differentiate between critical and non-critical functions. The BCP must clearly describe the types of events that would lead up to the formal declaration of a business disruption and the process for activating the BCP.**

OM-5.5.2 **The BCP must clearly identify alternate sites for different operations, the total number of recovery personnel, workspace requirements, and applications and technology requirements. Office facilities and records requirements must also be identified.**

OM-5.5.3 Licensees should take note that they might need to cater for processing volumes that exceed those under normal circumstances. The interdependency among critical services is another major consideration in determining the recovery strategies and priority. For example, the resumption of the front office operations is highly dependent on the recovery of the middle office and back office support functions.

OM-5.5.4 **Individual critical business and support functions must establish the minimum BCP recovery objectives for recovering essential business operations and supporting systems to a specified level of service ("recovery level") within a defined period following a disruption ("recovery time"). These recovery levels and recovery times must be approved by the senior management prior to proceeding to the development of the BCP.**

List of Contacts and Responsibilities

OM-5.5.5 **The BCP must contain a list of all key personnel. The list must include personal contact information on each key employee such as their home address, home telephone number, and cell phone or pager number so they may be contacted in case of a disaster or other emergency.**

OM-5.5 BCP – Recovery Levels & Objectives (continued)

OM-5.5.6 **The BCP must contain all the necessary process steps to complete each critical business operation or service. Each process must be explained in sufficient detail to allow another employee to perform the job in case of a disaster.**

Alternate Sites for Business and Technology Recovery

OM-5.5.7 Most business continuity efforts are dependent on the availability of an alternate site (i.e. recovery site) for successful execution. The alternate site may be either an external site available through an agreement with a commercial vendor or a site within the Licensee's real estate portfolio. A useable, functional alternate site is an integral component of BCP.

OM-5.5.8 **Licensees must examine the extent to which key business functions are concentrated in the same or adjacent locations and the proximity of the alternate sites to primary sites. Alternate sites must be sufficiently remote from, and do not depend upon the same physical infrastructure components as a licensee's primary business location. This minimises the risk of both sites being affected by the same disaster (e.g. they must be on separate or alternative power grids and telecommunication circuits).**

OM-5.5.9 **Licensees' alternate sites must be readily accessible and available for occupancy (i.e. 24 hours a day, 7 days a week) within the time requirement specified in their BCP. Should the BCP so require, the alternate sites must have pre-installed workstations, power, telephones and ventilation, and sufficient space. Appropriate physical access controls such as access control systems and security guards must be implemented in accordance with Licensee's security policy.**

OM-5.5.10 Other than the establishment of alternate sites, licensees should also pay particular attention to the transportation logistics for relocation of operations to alternate sites. Consideration should be given to the impact a disaster may have on the transportation system (e.g. closures of roads). Some staff may have difficulty in commuting from their homes to the alternate sites. Other logistics, such as how to re-route internal and external mail to alternate sites should also be considered. Moreover, pre-arrangement with telecommunication companies for automated telephone call diversion from the primary work locations to the alternate sites should be considered.

OM-5.5 BCP – Recovery Levels & Objectives (continued)

OM-5.5.11 Alternate sites for technology recovery (i.e. back-up data centres), which may be separate from the primary business site, should have sufficient technical equipment (e.g. workstations, servers, printers, etc.) of appropriate model, size and capacity to meet recovery requirements as specified by licensees' BCPs. The sites should also have adequate telecommunication (including bandwidth) facilities and pre-installed network connections as specified by their BCP to handle the expected voice and data traffic volume.

OM-5.5.12 Licensees should avoid placing excessive reliance on external vendors in providing BCP support, particularly where a number of institutions are using the services of the same vendor (e.g. to provide back-up facilities or additional hardware). Licensees should satisfy themselves that such vendors do actually have the capacity to provide the services when needed and the contractual responsibilities of the vendors should be clearly specified. Licensees should recognise that outsourcing a business operation does not transfer the associated business continuity management responsibilities.

OM-5.5.13 The contractual terms should include the lead-time and capacity that vendors are committed to deliver in terms of back-up facilities, technical support or hardware. The vendor should be able to demonstrate its own recoverability including the specification of another recovery site in the event that the contracted site becomes unavailable.

OM-5.5.14 Certain licensees may rely on a reciprocal recovery arrangement with other institutions to provide recovery capability (e.g. Cheque sorting and cash handling). Licensees should, however, note that such arrangements are often not appropriate for prolonged disruptions or an extended period of time. This arrangement could also make it difficult for Licensees to adequately test their BCP. Any reciprocal recovery agreement should therefore be subject to proper risk assessment and documentation by licensees, and formal approval by the Board.

OM-5.6 Detailed Procedures for the BCP

OM-5.6.1 Once the recovery levels and recovery objectives for individual business lines and support functions are determined, the development of the detailed BCP should commence. The objective of the detailed BCP is to provide detailed guidance and procedures in a crisis situation, of how to recover critical business operations or services identified in the Business Impact Analysis stage, and to ultimately return to operations as usual.

Crisis Management Process

OM-5.6.2 **A BCP must set out a Crisis Management Plan (CMP) that serves as a documented guidance to assist the CMT in dealing with a crisis situation to avoid spill over effects to the business as a whole. The overall CMP, at a minimum, must contain the following:**

(a) A process for ensuring early detection of an emergency or a disaster situation and prompt notification to the CMT about the incident;

(b) A process for the CMT to assess the overall impact of the crisis situation on the licensee and to make quick decisions on the appropriate responses for action (i.e. staff safety, incident containment and specific crisis management procedures);

(c) Arrangements for safe evacuation from business locations (e.g. directing staff to a pre-arranged emergency assembly area, taking attendance of all employees and visitors at the time and tracking missing people through different means immediately after the disaster);

(d) Clear criteria for activation of the BCP and/or alternate sites;

(e) A process for gathering updated status information for the CMT (e.g. ensuring that regular conference calls are held among key staff from relevant business and support functions to report on the status of the recovery process);

(f) A process for timely internal and external communications; and

(g) A process for overseeing the recovery and restoration efforts of the affected facilities and the business services.

OM-5.6 Detailed Procedures for the BCP (continued)

OM-5.6.3 If CMT members need to be evacuated from their primary business locations, the licensee should set up a command centre to provide the necessary workspace and facilities for the CMT. Command centres should be sufficiently distanced from the licensee's primary business locations to avoid being affected by the same disaster.

Business Resumption

OM-5.6.4 **Each relevant business and support function must assign at least one member to be a part of the CMT to carry out the business resumption process for the relevant business and supported function. Appropriate recovery personnel with the required knowledge and skills must be assigned to the team.**

OM-5.6.5 Generally, the business resumption process consists of three major phases:

(a) The mobilisation phase – This phase aims to notify the recovery teams (e.g. via a call-out tree) and to secure the resources (e.g. recovery services provided by vendors) required to resume business services.

(b) The alternate processing phase – This phase emphasizes the resumption of the business and service delivery at the alternate site and/or in a different way than the normal process. This may entail record reconstruction and verification, establishment of new controls, alternate manual processes, and different ways of dealing with customers and counterparties; and

(c) The full recovery phase – This phase refers to the process for moving back to a permanent site after a disaster. This phase may be as difficult and critical to the business as the process to activate the BCP.

OM-5.6.6 For the first two phases above, clear responsibilities should be established and activities prioritised. A recovery tasks checklist should be developed and included in the BCP.

Technology Recovery

OM-5.6.7 Business resumption very often relies on the recovery of technology resources that include applications, hardware equipment and network infrastructure as well as electronic records. The technology requirements that are needed during recovery for individual business and support functions should be specified when the recovery strategies for the functions are determined.

OM-5.6 Detailed Procedures for the BCP (continued)

OM-5.6.8 Licensees should pay attention to the resilience of critical technology equipment and facilities such as the uninterruptible power supply (UPS) and the computer cooling systems. Such equipment and facilities should be subject to continuous monitoring and periodic maintenance and testing.

OM-5.6.9 **Appropriate personnel must be assigned with the responsibility for technology recovery. Alternative personnel need to be identified as back up for key technology recovery personnel in the case of the latter unavailability to perform the recovery process.**

Disaster Recovery Models

OM-5.6.10 There are various disaster recovery models that can be adopted by licensees to handle prolonged disruptions. The traditional model is an "active/back-up" model, which is widely used by many organizations. This traditional model is based on an "active" operating site with a corresponding alternate site (back-up site), both for data processing and for business operations.

OM-5.6.11 A split operations model, which is increasingly being used by major institutions, operates with two or more widely separated active sites for the same critical operations, providing inherent back up for each other (e.g. branches). Each site has the capacity to take up some or all of the work of another site for an extended period of time. This strategy can provide nearly immediate resumption capacity and is normally able to handle the issue of prolonged disruptions.

OM-5.6.12 The split operations model may incur higher operating costs, in terms of maintaining excess capacity at each site and added operating complexity. It may also be difficult to maintain appropriately trained staff and the split operations model can pose technological issues at multiple sites.

OM-5.6.13 The question of what disaster recovery model to adopt is for individual licensees' judgment based on the risk assessment of their business environment and the characteristics of their own operations.

OM-5.7 Vital Records Management

OM-5.7.1 Each BCP must clearly identify information deemed vital for the recovery of critical business and support functions in the event of a disaster as well as the relevant protection measures to be taken for protecting vital information. Licensees must refer to Chapter OM-7 when identifying vital information for business continuity. Vital information includes information stored on both electronic and non-electronic media.

OM-5.7.2 Copies of vital records must be stored off-site as soon as possible after creation. Back-up vital records must be readily accessible for emergency retrieval. Access to back-up vital records must be adequately controlled to ensure that they are reliable for business resumption purposes. For certain critical business operations or services, licensees must consider the need for instantaneous data back up to ensure prompt system and data recovery. There must be clear procedures indicating how and in what priority vital records are to be retrieved or recreated in the event that they are lost, damaged or destroyed.

OM-5.8 Other Policies Standards, and Processes

Employee Awareness and Training Plan

OM-5.8.1 **Licensees must implement an awareness plan and business continuity training for employees to ensure that all employees are continually aware of their responsibilities and know how to remain in contact and what to do in the event of a crisis.**

OM-5.8.2 Key employees should be involved in the business continuity development process, as well as periodic training exercises. Cross training should be utilised to anticipate restoring operations in the absence of key employees. Employee training should be regularly scheduled and updated to address changes to the BCP.

Public Relations & Communication Planning

OM-5.8.3 **Licensees must develop an awareness program and formulate a formal strategy for communication with key external parties (e.g. CBB and other regulators, investors, customers, counterparties, business partners, service providers, the media and other stakeholders) and provide for the type of information to be communicated. The strategy needs to set out all the parties the licensee must communicate to in the event of a disaster. This will ensure that consistent and up-to-date messages are conveyed to the relevant parties. During a disaster, ongoing and clear communication is likely to assist in maintaining the confidence of customers and counterparties as well as the public in general.**

OM-5.8.4 **The BCP must clearly indicate who may speak to the media and other key external parties, and have pre-arrangements for redirecting external communications to designated staff during a disaster. Important contact numbers and e-mail addresses of key external parties must be kept in a readily accessible manner (e.g. in wallet cards or licensees' intranet).**

OM-5.8.5 Licensees may find it helpful to prepare draft press releases as part of their BCP. This will save the CMT time in determining the main messages to convey in a chaotic situation. Important conversations with external parties should be properly logged for future reference.

OM-5.8 Other Policies, Standards and Processes (continued)

OM-5.8.6 ~~As regards~~ With reference to internal communication, the BCP should set out how the status of recovery can be promptly and consistently communicated to all staff, parent bank, head office, branches and subsidiaries (where appropriate). This may entail the use of various communication channels (e.g. broadcasting of messages to mobile phones of staff, Licensees websites, e-mails, intranet and instant messaging).

Insurance and other Risk Mitigating Measures

OM-5.8.7 **Licensees must have proper insurance coverage to reduce the financial losses that they may face during a disaster. Licensees must regularly review the adequacy and coverage of their insurance policies in reducing any foreseeable risks caused by disasters (e.g. loss of offices, critical IT facilities and equipment).**

Government and Community

OM-5.8.8 Licensees may need to coordinate with community and government officials and the media to ensure the successful implementation of the BCP. This establishes proper protocol in case a city- wide or region- wide event impacts the licensee's operations. During the recovery phase, facilities access, power, and telecommunications systems should be coordinated with various entities to ensure timely resumption of operations. Facilities access should be coordinated with the police and fire department and, depending on the nature and extent of the disaster.

Disclosure Requirements

OM-5.8.9 **Licensees must disclose how their BCP addresses the possibility of a future significant business disruption and how the licensee will respond to events of varying scope. Licensees must also state whether they plan to continue business during disruptions and the planned recovery time. ~~The licensees might make these disclosures on their websites, or through mailing to key external parties upon request.~~ In all cases, BCP disclosures must be reviewed and updated to address changes to the BCP.**

OM-5.8.9A The licensees might make these disclosures on their websites, or through mailing to key external parties upon request.

OM-5.9 Maintenance, Testing and Review

Testing & Rehearsal

OM-5.9.1 A BCP is not complete if it has not been subject to proper testing. Testing is needed to ensure that the BCP is operable. Testing verifies the awareness of staff and the preparedness of differing departments/functions of the bank.

OM-5.9.2 **Licensees must test their BCPs at least annually. Senior management must participate in the annual testing, and demonstrate their awareness of what they are required to do in the event of the BCP being involved. Also, the recovery and alternate personnel must participate in testing rehearsals to familiarise themselves with their responsibilities and the back-up facilities and remote sites (where applicable).**

OM-5.9.3 **All of the BCP's related risks and assumptions must be reviewed for relevancy and appropriateness as part of the annual planning of testing. The scope of testing must be comprehensive enough to cover the major components of the BCP as well as coordination and interfaces among important parties. A testing of particular components of the BCP or a fully integrated testing must be decided or depending on the situation. The following points must be included in the annual testing:**

(a) Staff evacuation and communication arrangements (e.g. call-out trees) must be validated;

(b) The alternate sites for business and technology recovery must be activated;

(c) Important recovery services provided by vendors or counterparties must form part of the testing scope;

(d) Licensees must consider testing the linkage of their back up IT systems with the primary and back up systems of service providers;

(e) If back up facilities are shared with other parties (e.g. subsidiaries of the licensee), the licensee needs to verify whether all parties can be accommodated concurrently; and

(f) Recovery of vital records must be performed as part of the testing.

OM-5.9 Maintenance, Testing and Review (continued)

OM-5.9.4 Formal testing reviews of the BCP must be performed to assess the thoroughness and effectiveness of the testing. Specifically, a post-mortem review report must be prepared at the completion of the testing stage for formal sign-off by Licensees' senior management. If the testing results indicate weaknesses or gaps in the BCP, the plan and recovery strategies must be updated to remedy the situation.

Periodic Maintenance and Updating of a BCP

OM-5.9.5 Licensees must have formal procedures to keep their BCP updated with respect to any changes to their business. In the event of a plan having been activated, a review process must be carried out once normal operations are restored to identify areas for improvement. If vendors are needed to provide vital recovery services, there must be formal processes for regular ~~(say, annual)~~ annual review of the appropriateness of the relevant service level agreements.

OM-5.9.6 Individual business and support functions, with the assistance of the CMT, must review their business impact analysis and recovery strategy on an annual basis. This aims to confirm the validity of, or whether updates are needed to, the BCP requirements (including the technical specifications of equipment of the alternate sites) for the changing business and operating environment.

OM-5.9.7 The contact information for key staff, counterparties, customers and service providers must be updated as soon as possible when notification of changes is received.

OM-5.9 Maintenance, Testing and Review (continued)

OM-5.9.8 Significant internal changes (e.g. merger or acquisitions, business re-organisation or departure of key personnel) must be reflected in the plan immediately and reported to senior management.

OM-5.9.9 Copies of the BCP document must be stored at locations separate from the primary site. A summary of key steps to be taken in an emergency situation must be made available to senior management and other key personnel.

Audit and Independent Review

OM-5.9.10 The internal audit function of a licensee or its external auditors must conduct periodic reviews of the BCP to determine whether the plan remains realistic and relevant, and whether it adheres to the policies and standards of the licensee. This review must include assessing the adequacy of business process identification, threat scenario development, business impact analysis and risk assessments, the written plan, testing scenarios and schedules~~, and communication of test results and recommendations to the Board.~~

OM-5.9.11 Significant findings and recommendations must be brought to the attention of the Board and Senior Management within three months of the completion of the review. Furthermore, Senior Management and the Board must ensure that any gaps or shortcomings reported to them are addressed in an appropriate and timely manner.

OM-5.10 Cyber Security Risk Management

OM-5.10.1 To prepare for the eventuality of cyber attacks, licensees must have a cyber attack response mechanism in place as part of the overall cyber risk strategy. The BCP of the licensee must also be properly enhanced to account for all CBB requirements and must be regularly tested to ensure ~~assure~~ that the licensee is capable of dealing with cyber attacks that will trigger the business continuity plans.

OM-6.1 Physical Security Measures for Retail Banks

General Requirement

OM-6.1.1 **Retail banks must maintain up to date Payment Card Industry Data Security Standards (PCI-DSS) certification. ~~This initial certification must be obtained by 30th April 2017.~~ Failure to comply with this requirement will trigger a supervisory response, which may include formal enforcement measures, as set out in Module EN (Enforcement).**

OM-6.1.1.A In order to maintain up to date PCI-DSS certification, retail banks will be periodically audited by PCI authorised companies for compliance. Licensees are asked to make certified copies of such documents available if requested by the CBB.

External Measures

OM-6.1.2 **All head offices are required to maintain Ministry of Interior ("MOI") guards on a 24 hours basis. All branches must maintain a 24 hour MOI guard. However, if branches satisfy the criteria mentioned in Paragraphs OM-6.1.3 to OM-6.1.22 below, they may maintain MOI guards during opening hours only. Furthermore, banks will be allowed to replace MOI armed guards with private security guards subject to the approval of the MOI. Training and approval of private security guards will be given by the MOI. Head Offices must always have a 24 hour MOI guard.**

OM-6.1.3 **Public entrances to head offices and branches must be protected by measures such as steel rolling shutters, or the external doors must be of solid steel or a similar solid material of equivalent strength and resistance to fire. Other external entrances must have steel doors or be protected by steel rolling shutters. Preferably, all other external entrances must have the following security measures:**

(a) Magic eye;
(b) Locking device (key externally and handle internally);
(c) Door closing mechanism;
(d) Contact sensor with alarm for prolonged opening time; and
(e) Combination access control system (e.g. access card and key slot or swipe card and password).

If additional security measures such as security cameras, motion detectors or intruder alarms are installed, the requirement for steel external doors or protection by steel rolling shutters is waived.

~~OM-6.1.4~~

[This Paragraph was deleted in March 2019 and requirements are now covered under Paragraph OM-6.1.3.] ~~Other external entrances must have steel doors or be protected by steel rolling shutters. Preferably, all other external entrances must have the following security measures:~~

~~(a) Magic eye;~~

~~(b) Locking device (key externally and handle internally);~~

~~(c) Door closing mechanism;~~

~~(d) Contact sensor with alarm for prolonged opening time; and~~

~~(e) Combination access control system (e.g. access card and key slot or swipe card and password).~~

OM-6.1 Physical Security Measures for Retail Banks (continued)

OM-6.1.5 [This Paragraph was deleted in March 2019 and requirements are now covered under Paragraph OM-6.1.3.] ~~If additional security measures to those mentioned in OM-6.1.3 and OM-6.1.4 such as security cameras, motion detectors or intruder alarms are installed, the requirement for steel external doors or protection by steel rolling shutters is waived.~~

OM-6.1.6 External windows must have security measures such as anti blast films and movement detectors. For ground floor windows, banks may also wish to add steel grills fastened into the wall.

OM-6.1.7 Branch alarm systems should have the following features:

(a) PIR motion detectors
(b) Door sensors
(c) Anti vibration/movement sensors on vaults
(d) External siren
(e) The intrusion detection system must be linked to the bank's (i.e. head office) monitoring unit and also the MOI Central Monitoring Unit.

Internal Measures

OM-6.1.8 Teller counters must be screened off from customers by a glass screen of no less than 1 meter in height from the counter work surface or 1.4 meters from the floor.

OM-6.1.9 All areas where cash is handled must be screened off from customers and other staff areas.

OM-6.1.10 Access to teller areas must be restricted to authorised staff only. The design of the teller area must not allow customers to pass through it.

OM-6.1.11 Panic alarm systems for teller staff must be installed. The choice between silent or audible panic alarms is left to individual banks. Kick bars and/or hold up buttons must be spread throughout the teller and customer service areas and the branch manager's office. The panic alarm must be linked to the MOI Central Monitoring Unit.

OM-6.1 Physical Security Measures for Retail Banks (continued)

Cash Safety

OM-6.1.12 Cash precious metals and bearer instruments must be kept in fireproof cabinets/safes. Preferably, these cabinets/safes must be located in strong rooms.

OM-6.1.13 Strong rooms must be made of reinforced solid concrete, or reinforced block work. Doors to strong rooms must be steel and preferably also have a steel shutter fitted. Dual locking devices must be installed in strong room doors. Strong room doors must be located out of the sight of customers.

OM-6.1.14 Strong rooms must not contain any other openings except the entry door and where necessary, an air conditioning outlet. The air conditioning outlet must be protected with a steel grill.

OM-6.1.15 [This Paragraph was deleted in April 2016.]

OM-6.1.16 [This Paragraph was deleted in April 2016 and requirements were moved to Section OM-6.4.]

OM-6.1.17 [This Paragraph was deleted in April 2016.]

OM-6.1.18 [This Paragraph was deleted in April 2016 and requirements were moved to Section OM-6.4.]

OM-6.1.19 [This Paragraph was deleted in April 2016 and requirements are now covered under Paragraph OM-6.4.14.]

OM-6.1 Physical Security Measures for Retail Banks (continued)

CCTV Network Systems

OM-6.1.20 All head offices and branches must have a CCTV network and alarm system which are connected to a central monitoring unit located in the head office, along with a Video Monitoring System (VMS) and to the MOI Central Monitoring Unit.

OM-6.1.21 At a minimum, CCTV cameras must cover the following areas:

(a) Main entrance;
(b) Other external doors;
(c) Any other access points (e.g. ground floor windows);
(d) The banking hall;
(e) Tellers' area;
(f) Strong room entrance; and
(g) ATMs (by way of internal or external cameras) Refer to Section OM-6.3 for specific CCTV requirements related to ATMs.

OM-6.1.22 Notices of CCTV cameras in operation must be put up for the attention of the public. CCTV records must be maintained for a minimum 45-day period. The transmission rate (in terms of the number of frames per second) must be high enough to make for effective monitoring. Delayed transmission of pictures to the Central Monitoring Unit is not acceptable. The CCTV system must be operational 24 hours per day.

OM-6.1 Physical Security Measures for Retail Banks (continued)

Training and Other Measures

OM-6.1.23 Banks must establish the formal position of security manager. This person will be responsible for ensuring all bank staff are given annual, comprehensive security training. Banks must produce a security manual or procedures for staff, especially those dealing directly with customers. For banks with three or more branches, this position must be a formally identified position. For banks with one or two branches, the responsibilities of this position may be added to the duties of a member of management.

OM-6.1.24 The security manager must maintain records on documented security related complaints by customers and take corrective action or make recommendations for action on a timely basis. Actions and recommendations must also be documented.

OM-6.1.25 Banks must consider safety and security issues when selecting premises for new branches. Key security issues include prominence of location (i.e. Is the branch on a main street or a back street?), accessibility for emergency services, and assessment of surrounding premises (in terms of their safety or vulnerability), and the number of entrances to the branch. All banks are required to hold an Insurance Blanket Bond (which includes theft of cash in its cover).

OM-6.1.26 [This Paragraph was deleted in March 2019.] ~~Further rules on ATM Physical Security Measures are contained in Section OM-6.4.~~

MODULE	OM:	Operational Risk Management
CHAPTER	OM-6:	Security Measures for Banks

OM-6.2 Internet Security for all Banks

OM-6.2.1 All banks providing internet banking services must regularly test their systems against security breaches and verify the robustness of the security controls in place. These tests must be conducted by security professionals, such as ethical hackers, that provide penetration testing services and a vulnerability assessment of the system. The tests must be undertaken by external independent parties that are not employees of the bank nor associated with it.

OM-6.2.2 The penetration testing referred to in Paragraph OM-6.2.1, must be conducted each year in June and December.

OM-6.2.3 The vulnerability assessment report, along with the steps taken to mitigate the risks must be maintained by the bank for a 5-year period from the date of testing and must be provided to the CBB within two months following the end of the month where the testing took place, i.e. for the June test, the report must be submitted at the latest by 31st August and for the December test, by 28th February (see Section BR-4A.2).

OM-6.3 ATM Security Measures: Hardware/Software for Retail Banks

~~*Implementation*~~

OM-6.3.1 [This Paragraph was deleted in March 2019] ~~The requirements in this Section must be complied with in full by 30th April 2017, or as specified otherwise. Failure to comply with these requirements will trigger a supervisory response, which may include formal enforcement measures, as set out in Module EN (Enforcement).~~

Europay, MasterCard and Visa (EMV) Compliance

OM-6.3.1A All cards (debit, credit, charge, prepaid, etc.) issued by licensees in the Kingdom of Bahrain must be EMV compliant. Moreover, all ATMs, CDMs, POS, etc. must be EMV compliant for accepting cards issued in the Kingdom of Bahrain. In this context, EMV compliant means using chip and online PIN authentication. However, contactless card payment transactions, where no PIN verification is required, are permitted for small amounts i.e. up to BD 20 per transaction, provided that Islamic bank licensees bear full responsibility in case of fraud occurrence.

Provision of Cash Withdrawal and Payment Services through Various Channels

OM-6.3.1B Islamic bank licensees are allowed to provide cash withdrawal and payment services using various channels, including but not limited to, contactless, cardless, QR code, e-wallets, biometrics (iris recognition, facial recognition, fingerprint, voiceprint, etc.), subject to enrolling customers through registration process wherein customers' acceptance of products/services terms and conditions are documented and customers are properly authenticated.

Geolocation Limitations

OM-6.3.2 All Islamic bank licensees issuing debit, prepaid and/or credit cards must ensure that all Bahrain issued cards enable each customer to maintain a list of 'approved' countries for card ATM/Point of Sale (POS) transactions. Customers must be allowed to determine those countries in which their cards must not be accepted as well as countries or merchant categories in which a card transaction would require a further level of authorisation, (for example, 2-way SMS).

MODULE	OM:	Operational Risk Management
CHAPTER	OM-6:	Security Measures for Banks

OM-6.3 ATM Security Measures: Hardware/Software for Retail Banks continued

Prohibition of Double Swiping

OM-6.3.2A **Double swiping of cards by merchants is not allowed, and all card acquirer licensees must ~~communicate to~~ ensure that the ~~concerned~~ merchants concerned ~~that the CBB has directed to stop the practice of double swiping of payment cards by some merchants at the merchant's POS terminals/ECR, with effect from 15th June, 2017.~~comply with this requirement.**

OM-6.3.2B For the purpose of Paragraph OM-6.3.2A, card acquirer licensee means a CBB licensee that enters into a contractual relationship with a merchant and the payment card issuer, under a card payment scheme, for accepting and processing payment card transactions. Card acquirers include three-party payment card network operators, who have outsourced their acquiring services to third party service providers.

OM-6.3.2C For the purpose of Paragraph OM-6.3.2A, double swiping means swiping of a payment card by a merchant at the POS terminal/ECR for the second time, resulting in capturing and storing of payment cardholder data and sensitive authentication data encoded on the magnetic stripe of a customer's payment card, after the merchant received the required card payment authorisation response.

OM-6.3 ATM Security Measures: Hardware/Software for Retail Banks (continued)

OM-6.3.2D All card acquirer licensees must include the following clause into the merchant agreements entered into with all their merchants ~~and bring into force the said clause on or before 15th June, 2017~~: "Pursuant to the CBB directions and instructions, the merchant shall stop double swiping of a payment card at a merchant's point-of-sale (POS) terminal/electronic cash register (ECR) to capture or store cardholder and sensitive authentication data encoded on the magnetic stripe of a customer's payment card, after the merchant received the required card payment authorisation response. The merchant asserts its full compliance with the obligation contained in this clause and understands that any breach of this clause will expose the merchant to mandatory contractual and/or legal disciplinary actions by the relevant regulator and/or concerned Ministry."

OM-6.3.2E All card acquirer licensees must:

(i) Educate the concerned merchants on the regulatory requirement and continue to follow up the progress of the implementation to comply within the period stipulated in Paragraph OM-6.3.2A; and

(ii) Educate and facilitate, where necessary, any merchant that has a valid business need to have cardholder data or non-sensitive information, to transmit such data/information through an integration option.

Integration of Hardware Components

OM-6.3.3 If the Automated Teller Machines (ATM) environment permits access to internal areas where account data is processed and/or stored (e.g., for service or maintenance), these areas must be effectively protected from access by unauthorised persons to mitigate the risk associated with attaching/inserting malicious additional components, especially those which may be designed to capture sensitive data. Banks must encrypt account data or secure access to such data by effective physical barriers such as strong walls, doors, and mechanical locks.

OM-6.3.4 All entry to sensitive areas must be recorded, including the name of the persons accessing the area; the date; and the time of access to and exit from the area. CCTV cameras must be installed, and used to record all activities within the ATM environment.

OM-6.3 ATM Security Measures: Hardware/Software for Retail Banks (continued)

OM-6.3.5 Banks are required to implement best industry practice in respect of hardware and software development and integration, including but not limited to formal specification, test plans, and documentation. Hardware and software should only be introduced to the environment following a successful programme of testing.

OM-6.3.6 All test plans and the outcomes of these plans must be retained by the bank for a minimum of five years from the date of testing and be available on request to the CBB or their authorised representatives. Examples of instances in which a detailed testing process must be undertaken prior to installation and integration of components include, but are not limited to, secure card readers or EPPs. In all instances the applicable standards relating to Payment Card Industry (PCI), PIN Transaction Security (PTS), and Point of Interaction (POI) requirements must be fully complied with.

OM-6.3.7 Banks must ensure that the integration of Secure Card Readers, (SCRs) and, if applicable, any mechanism protecting the SCRs are properly implemented and fully comply with the guidelines provided by the device vendor. SCRs must be PCI Security Standards Council approved ~~by~~ and fully comply with all ~~Payment Card Industry~~ PCI standards at all times.

OM-6.3.8 Banks must ensure that all ATMs, including offsite ATMs, are equipped with mechanisms which prevent skimming attacks. There must be no known or demonstrable way to disable or defeat the above-mentioned mechanisms, or to install an external or internal skimming device.

ATM Software

OM-6.3.9 Banks must ensure that their ATM software security measures comply with the following:

(a) Access to sensitive services is controlled by requiring authentication. Entering or exiting sensitive services must not reveal or otherwise compromise the security of sensitive information;

OM-6.3 ATM Security Measures: Hardware/Software for Retail Banks (continued)

(b) ATM software must include controls which are designed to prevent unauthorised modification of the software configuration, including the operating system, drivers, libraries, and individual applications. Software configuration includes the software platform, configuration data, applications loaded to and executed by the platform, and the associated data. The mechanisms must also ensure the integrity of third-party applications, using a controlled process to install such controls;

(c) Access to all elements of the ATM environment must be strictly controlled to ensure an effective segregation of functions and an effective segregation of responsibilities exists for all personnel; ~~and~~

(d) The logging data must be stored in a way that data cannot be changed under any circumstances, and deleted only after authorisation by a member of bank staff who has specific responsibility delegated by the CEO;

(e) Software is protected and stored in a manner which precludes unauthorised modification; and

(f) Loading of software into ATMs is performed by a person who has the requisite knowledge and skills, and who has been nominated and authorised by a senior manager in the bank to undertake these tasks.

OM-6.3.10 ATMs ~~should~~ must incorporate dedicated tampering protection capabilities.

Device Management/Operation

OM-6.3.11 [This Paragraph was deleted in March 2019 and requirements are now covered under Paragraph OM-6.3.9.]~~Banks must ensure that their device management/operation controls comply with the following:~~

~~(a) Software is protected and stored in a manner which precludes unauthorised modification; and~~

~~(b) Loading of software into ATMs is performed by a person who has the requisite knowledge and skills, and who has been nominated and authorised by a senior manager in the bank to undertake these tasks.~~

OM-6.3 ATM Security Measures: Hardware/Software for Retail Banks (continued)

ATM Application Management

OM-6.3.12 Banks must ensure that their ATM application management complies with the following:

(a) The display of a cardholder PIN must be obfuscated on the ATM display and must not be in 'clear' mode;

(b) Sensitive information must not be present any longer or used more often than strictly necessary. The ATM must automatically clear its internal buffers when either the transaction is completed, or the ATM has timed out whilst awaiting a response from the cardholder or host; and

(c) Prevent the display or disclosure of cardholder account information such as the account number, ID number, address and other personal details etc. on the ATM screen, printed on receipts, or audio transcripts for visually impaired cardholders.

OM-6.4 ATM Security Measures: Physical Security for Retail Banks

~~*Implementation*~~

OM-6.4.1 [This Paragraph was deleted in March 2019] ~~The requirements in this Section must be complied with in full by 31st March 2017. Failure to comply with any of these requirements will trigger a supervisory response, which may include formal enforcement measures, as set out in Module EN (Enforcement).~~

Record Keeping

OM-6.4.2 Banks must record the details of the site risk assessments and retain such records for a period of five years from the date of the ATM installation, or whatever other period required by the Ministry of the Interior or the CBB from time to time, whichever is the longer.

Installation of an Off-site ATM in Bahrain

OM-6.4.3 Applications for the installation of off-site ATMs must be sent in writing, and in accordance with the requirements set out in Paragraphs OM-6.4.6 to Paragraphs OM-6.4.12 to the Supervisory Point of Contact (SPoC), at the CBB.

OM-6.4.4 The purpose of the content of Paragraphs OM-6.4.5 to OM-6.4.12 is to set out the minimum criteria to be followed by banks for the installation and usage of off-site ATMs in the Kingdom of Bahrain.

General Criteria

OM-6.4.5 The ownership and operations of any off-site ATMs is subject to the prior written approval of the CBB and banks must comply with the Rules outlined in Paragraphs OM-6.4.6.

OM-6.4.6 Off-site ATMs must be owned either individually or jointly by banks or ancillary service providers which are members of the BENEFIT Switch. Each relevant owning bank must already have linked its ATM capability to the BENEFIT Switch prior to requesting the CBB's permission to install an off-site ATM and, furthermore, must conform to the general standards set by the ~~Benefit~~ BENEFIT Company from time to time or by the ancillary service provider licensed by the CBB.

OM-6.4.7 Banks must bear full legal responsibility for their respective off-site ATMs, as well as all costs associated with such ATMs (including, but not limited to, cash replenishment, installation, security etc.).

OM-6.4 ATM Security Measures: Physical Security for Retail Banks (continued)

OM-6.4.8 **Banks wishing to install an off-site ATM must submit an application (in writing) for the CBB's approval (see Paragraph BR-5.3.3). A copy of the written permission (for installation of that off-site ATM) of the legal owner of the proposed location must be provided to the CBB, as well as a copy of the written permission of any other relevant authorities in this context ~~(e.g. the Ministry of Interior).~~**

OM-6.4.9 The CBB will consider applications on a 'first come, first served' basis for a particular location. If more than one application is received to install an off-site ATM in the same location, the number of such applications which are approved will depend upon whether the location appears to the CBB to be capable of sustaining multiple off-site ATMs subject to the exact details of each individual application regarding security being acceptable to the CBB.

OM-6.4.10 Each application will be assessed on its individual merits, and at the CBB's sole discretion, taking into account factors which the CBB considers relevant including, but not limited to:

(a) The suitability of the location in question;
(b) The level of overall activities of the applicant in the market as well as the size and make-up of its customer base; and
(c) The type and range of facilities which the applicant proposes offering through the off-site ATM at the location in question.

OM-6.4.11 In addition to the information required by the CBB under Paragraph OM-6.4.8, the CBB may require further information/clarification to be provided to it before it takes a decision regarding the application. The CBB's decision in this regard will be notified to each relevant applicant bank in writing.

OM-6.4.12 **A bank must request in writing the CBB's permission to ~~close~~ remove/terminate any of its off-site ATMs.**

OM-6.4.13 The CBB may, at its sole discretion, require an off-site ATM to be ~~closed~~ removed/terminated and decommissioned at any time.

OM-6.4 ATM Security Measures: Physical Security for Retail Banks (continued)

ATM Alarms

OM-6.4.14 In addition to alarming the premises, banks must alarm the ATM itself, in a way which activates audibly when the ATM is under attack. The system must be monitored by remote signaling to an appropriate local police response designated by the Ministry of ~~the~~Interior. In doing so, banks must consider the following:

(a) The design of the system must ensure that the ATM has a panic alarm installed;

(b) The design of the system must give an immediate, system controlled warning of an attack on the ATM, and all ATMs must be fitted with fully operational fraud detection and inhibiting devices;

(c) A maintenance record must be kept for the alarm detection system and routine maintenance must be conducted in accordance with at least the manufacturer's recommendations. The minimum must be two planned maintenance visits and tests every 6 months; and

(d) The alarm system must be monitored from an Alarm Receiving Centre 24 hours daily. It must automatically generate an alarm signal if the telephone/internet line fails or is cut.

OM-6.4 ATM Security Measures: Physical Security for Retail Banks (continued)

Closed-circuit Television (CCTV)

OM-6.4.15 Banks must ensure that ATMs are equipped with Closed-circuit television (CCTV). The location of camera installation must be carefully chosen to ensure that images of the ATM are recorded, however keypad entries ~~are~~ must not be recorded. The camera must support the detection of the attachment of alien devices to the fascia (external body) and possess the ability to generate an alarm for remote monitoring if the camera is blocked or otherwise disabled.

OM-6.4.15A For the purposes of Paragraph OM-6.4.15, the location of camera installation in drive-thru ATMs must be carefully chosen to ensure that the images of the vehicle number plates are clearly captured during both daytime and nighttime.

OM-6.4.16 As a minimum, CCTV activity must be recorded (preferably in digital format) and, where risk dictates, remotely monitored by a third party ~~ARC~~ Alarm Receiving Centre.

OM-6.4.17 When an ATM is located in an area where a public CCTV system operates, the deployer or agent must liaise with the agency responsible for the CCTV system to include the ATM site in any preset automatic camera settings or to request regular sweeps of the site. The CCTV system must not be able to view the ATM keypad thereby preventing observation of PIN entry.

OM-6.4.18 Banks must ensure that the specifications of CCTV cameras meet the following minimum requirements:

(a) Analogue Cameras:
Resolution – Minimum 700 TVL
Lens – Vari-focal lenses from 2.8 to 12mm
Sensitivity – Minimum 0.5 Luminance (Lux) without Infrared (IR), 0 Lux with IR
IR – At least 10 to 20 meters (Camera that detects motion)

(b) IP Cameras:
Resolution – 2 MP – 1080 p
Lens – Vari-focal lenses from 2.8 to 12mm
Sensitivity – Minimum 0.5 Lux without IR, 0 Lux with IR
IR – At least 10 to 20 meters

OM-6.4 ATM Security Measures: Physical Security for Retail Banks (continued)

OM-6.4.19 Banks must ensure that the following network requirements are met for connecting the Banks CCTV system to MOI Control room:

(a) The minimum speed of the upload should be 2 Mbps for each node (ATM's and branches);

(b) Speed/storage limit threshold must not be applied in a manner which permits a network delay; and

(c) Access must be restricted to authorised personnel.

ATM Lighting

OM-6.4.20 Banks must ensure that adequate and effective lighting is operational at all times within the ATM environment. The standard of the proposed lighting must be agreed with the Ministry of the Interior and other relevant authorities, and tested at least once every three months to ensure that the lighting is in good working order.

OM-6.4.20A Banks must ensure that adequate and effective lighting is operational within drive-thru ATMs to enable the CCTV cameras to capture the vehicle number plates ~~at~~ during both daytime and nighttime.

OM-6.4.21 This Paragraph was deleted in July 2017

OM-6.4.22 This Paragraph was deleted in April 2017.

OM-6.4.23 This Paragraph was deleted in April 2017.

Fire Alarm

OM-6.4.24 Banks must ensure that effective fire alarm and fire defense measures, such as a sprinkler, are installed and functioning for all ATMs. These alarms must be linked to the "General Directorate of Civil Defense" in Bahrain.

OM-6.4 ATM Security Measures: Physical Security for Retail Banks (continued)

Cash Replenishment

OM-6.4.25 All cash movements between branches, to and from the CBB and to off-site ATMs must be performed by specialised service providers.

ATM Service/ Maintenance

OM-6.4.26 Banks must maintain a list of all maintenance, replenishment and inspection visits by staff or other authorised parties.

OM-6.5 ATM Security Measures: Additional Measures for Retail Banks

OM-6.5.1 Banks may ensure the adequacy and effectiveness of external security measures throughout the ATM environment through the additional security measures outlined in this Section.

Sounders and Flashing Warning Lights

OM-6.5.2 Banks should ensure that street-based ATMs are installed with an audible alarm sounder, and a visual flashing warning light, to indicate when the ATM is under attack.

Armored Anti-Bandit Shroud

OM-6.5.3 Banks should obtain and act upon advice provided by the Ministry of Interior in respect of protecting the ATM installation with an armored anti-bandit shroud which is placed around the ATM to prevent any bombing or other physical attempts to damage the ATM.

OM-6.6 Cyber Security Measures

OM-6.6.1 **Clear ownership and management accountability of the risks associated with cyber attacks and related risk management must be established, which cover not only the IT function but also all relevant business lines. Cyber security must be made part of the licensee IT security policy.**

OM-6.6.1A As part of the operational risk management process, a licensee should take into account and document the relevant cyber security risks. Moreover, in all matters concerning business continuity management, the licensee should also address cyber incident scenarios that could potentially affect its business activity, suppliers and service providers, the availability of supporting infrastructures, etc.

OM-6.6.1B Adequate management of cyber security risks requires augmentation of the licensee's existing information technology (IT) risk management framework, from the perspectives of threat landscape perception and the required security capabilities, as detailed in this Section.

Training

OM-6.6.1C **The licensee must ensure that all employees receive adequate training on a regular basis, in relation to cyber security and the threats they could encounter, such as through testing employee reactions to simulated cyber attack scenarios. All relevant employees must be informed on the current cyber security breaches and threats. Additional training should be provided to 'higher risk staff'.**

Role of Board and Senior Management

OM-6.6.2 **The Board and senior management must ensure that the cyber security controls are periodically evaluated for adequacy and effectiveness, taking into account emerging cyber threats and establishing a credible benchmark of cyber security controls endorsed by the Board and senior management. Should material gaps be identified, the Board and senior management must ensure that corrective action is taken immediately.**

OM-6.6.2A **The Board must be responsible for:**

(a) Setting and approving a corporate-wide cyber risk strategy;
(b) Approving a cyber risk management framework and a corporate-wide cyber defence policy;
(c) Determining the manner in which it oversees senior management with regard to the implementation of the cyber risk management framework; and ensure that the cyber roles within the organisation have been aligned to the overall cyber risk strategy.
(d) Receiving reports on significant cyber incidents.

OM-6.6 Cyber Security Measures (Continued)

OM-6.6.2B The senior management must be responsible for the following activities:

(a) Create an overall cyber risk management framework and adequately oversee its implementation;
(b) Formulate a corporate-wide cyber defence policy;
(c) Implement and consistently maintain an integrated, corporate-wide, cyber risk management framework, including sufficient resource allocation;
(d) Monitor the effectiveness of the implementation of cyber risk management practices and coordinate cyber defence activities with internal and external risk management entities;
(e) Receive periodic reports on the current situation with respect to cyber threats and cyber risk treatment from the relevant departments; and
(f) Receive periodic reports on all cyber incidents (internal and external) and analysis of their implications on the bank.
(g) Ensure that processes for identifying critical internal functions are in place and annually verified.

OM-6.6.2C Cyber security must be an item for discussion at Board meetings.

OM-6.6.2D The Board must ensure that the cyber security policy and procedures are robust and can comprehensively assist the bank's cyber security requirements. In the case of branches, it is recommended that there is a formal sign-off of a localised version of such a policy.

OM-6.6.2E A clear reporting line to the Board must be established for cyber security incidents. A dedicated IT Security Officer must be appointed with responsibility for cyber and information security.

Security Breach

~~OM-6.6.3~~ Licensees must report to the CBB within one week any instances of cyber attacks, whether internal or external, that compromise customer information or disrupt critical services that affect their operations. When reporting such instances, licensees must provide the root cause analysis of the cyber attack and measures taken by them to ensure that similar events do not recur.

OM-6.6 Cyber Security Measures (Continued)

Cyber Security Strategy

OM-6.6.4 A corporate-wide cyber security strategy must be defined and documented, which includes:

(a) The position and importance of cyber defence at the bank;
(b) The cyber-threat concept and the challenges facing the bank;
(c) The bank's approach to cyber risk management, definition and oversight the level of exposure to cyber threats; and
(d) The key elements of cyber defence strategy – objectives, principles of operation and implementation.

OM-6.6.4A The cyber security strategy should be revised as necessary and in any case, at least once every three years.

Cyber Risk Management Framework

OM-6.6.5 A cyber risk management framework should be defined and documented, which includes:

a) Identification of the corporate governance elements for cyber risk management, including areas of responsibility and reporting lines.
b) Detailed definition of tools and methodologies for the evaluation of risks and the manner in which they are implemented;
c) Detailed definition of main cyber security processes and measures and the manner of their control and assessment.

Cyber Security Policy

OM-6.6.6 Licensees must establish a cyber-security policy, which includes:

(a) Cyber defence objectives, definition of areas of responsibilities, involved positions and functions (including work interfaces);
(b) Organisational structures, structure and governance of the cyber risk management process at the bank;
(c) Internal procedural framework of the bank, details of the controls required and the framework for their implementation;
(d) Monitoring and responses, training and awareness, information gathering, research and sharing;
(e) Process maturity and effectiveness metrics and indexes; and
(f) Evaluation, control and reporting.

OM-6.6 Cyber Security Measures (Continued)

OM-6.6.6A The cyber security policy should be reviewed annually and should be revised as necessary.

OM-6.6.7 **The cyber security strategy, framework and policy will be reviewed by the CBB's on-site examination team or may be requested by the CBB for supervision purposes.**

OM-6.6.8 **Licensees must conduct a periodic assessment of cyber threats For the purpose of analysing and assessing cyber threats, the licensee should take into account the factors detailed below:**

a) Surveys and audit findings, and all current information that could be indicative of weaknesses in the relevant controls;

b) Collection and analysis of external data that could be indicative of potential vulnerabilities or lead to the detection of risk exposures that were not identified in the past;

c) Collection and analysis of data regarding cyber incidents within the licensee;

d) Mapping of business processes for the purpose of exposing specific risks, interdependencies between risks, and areas of weakness in controls or risk management;

e) Use of metrics for the purpose of quantifying the exposure to cyber risks, use of qualitative and/or quantitative assessment indicators, in a manner that should make it possible to monitor changes in these values from time to time.

f) Use of Key Risk Indicators (KRIs) and Key Process Indicators (KPIs), in order to provide insights on the status of control mechanisms and the cyber security program.

g) Analysis of scenarios, in licensee with business line managers and risk managers in order to detect potential incidence of risk materialization, to assess their potential impact, and to enhance the ability to detect and respond to those incidents;

MODULE	OM:	Operational Risk Management
CHAPTER	OM-6:	Security Measures for Banks

OM-6.6 Cyber Security Measures (Continued)

OM-6.6.9 Licensees must conduct a periodic assessment of cyber defence controls. Cyber defence control assessment must include an analysis of the controls' current status vis-à-vis relevant cyber threats, weaknesses and risks across the different activity segments, including:

(a) Physical access, administration and organization;
(b) Information system life cycle in various operational environments;
(c) Technology management and critical supporting systems;
(d) Interaction with customers, devices used by customers;
(e) Remote access, messaging and communication;
(f) Identity and access management, business partners and suppliers, information and data exchange channels; and
(g) Organisational culture and awareness, online presence, online banking and use of social networks, and business continuity.

OM-6.6.10 Licensees must arrange to seek cyber risk insurance cover from a suitable insurer, once the assessment of cyber security risk is complete. The insurance policy may include some or all of the following types of coverage, depending on the risk assessment outcomes.

(a) Crisis management expenses, such as costs of notifying affected parties, costs of forensic investigation, costs incurred to determine the existence or cause of a breach, regulatory compliance costs, costs to analyse the insured's legal response obligations;
(b) Claim expenses such as costs of defending lawsuits, judgments and settlements, and costs of responding to regulatory investigations; and
(c) Policy also provides coverage for a variety of torts, including invasion of privacy or copyright infringement. First-party coverages may include lost revenue due to interruption of data systems resulting from a cyber or denial of service attack and other costs associated with the loss of data collected by the insured.

MODULE	OM:	Operational Risk Management
CHAPTER	OM-6:	Security Measures for Banks

OM-6.6 Cyber Security Measures (Continued)

Cyber Security Monitoring

OM-6.6.11 **The licensee must establish an effective monitoring system, which receives data in real time from the various systems, including operational and business systems, and identifies indicators of cyber incidents, and initiates reporting and response activities as necessary.**

OM-6.6.12 The licensee should determine the period of time necessary for retaining the information required for detecting cyber incidents, including "low-and-slow" attacks, in order to facilitate incident investigations.

OM-6.6.13 **The monitoring systems must be integrated with other systems at the licensee in order to enable an effective cyber incident detection and response mechanism, including: detection of indicators of abnormal activity, information retrieval and enrichment, investigation and documentation, knowledge management and decision making, generation and management of alerts and reports, communication with relevant entities, and real time change management.**

OM-6.6.14 The licensee should periodically examine cyber incident scenarios for the purpose of assessing its ability to detect them and respond, and should update the monitoring and detection systems accordingly.

OM-6.6.15 **Licensee must have suitable processes in place to verify the validity of all requests received through all methods of communication, including email such as a phish alert solution. Banks must also ensure that mobile devices with access to their systems, applications and networks are protected through security measures, such as mobile device management, encryption, remote wipe and password protection.**

Exercises

OM-6.6.16 **Licensee must define a program for exercising the various response mechanism, taking into account the various types of exercises such as attack simulations, "war games" and "table top" exercises, and with reference to the relevant stakeholders such as technical staff, crisis management team, decision-makers, and spokespersons.**

OM-6.6 Cyber Security Measures (Continued)

Cyber Incident Management

OM-6.6.17 **In the course of cyber incident management, the licensee must identify the current stage of the incident and should handle it according to its characteristics. A cyber incident should be regarded as concluded only after it has been handled throughout its lifecycle.**

OM-6.6.18 **The licensee must define procedures for cyber incident management, including alerting, reporting, handling, responding and concluding, in accordance to its severity and stages.**

OM-6.6.19 For the purpose of managing a cyber-incident, the licensee should operate a situation room, and should define the authorities and responsibilities of staff members, internal and external reporting lines, communication channels, tools and detailed working procedures.

OM-6.6.20 The licensee should record and document in an orderly manner the incidents that have been handled and the actions that were taken by the relevant functions. In particular, the corporation should maintain an "incidents log" in which all the notifications, decisions and actions taken, in relation to cyber incidents, are documented, as close as possible to the time of their occurrence.

OM-6.6.21 **The licensee must define a pool of response activities (such as configuration change, restriction and/or diversion of communications, and deployment of software) in accordance with the different scenarios. In addition, the licensee must also define the conditions in which these response activities should be employed, the communication channels, the required approvals, and assessment of their effectiveness in the context of a given incident.**

OM-6.6.22 **The licensee must define a scale of alert levels, and the required activities in accordance with various alert levels, such as: prediction of an organized attack, the volume and severity of detected attacks within the licensee, the banking sector or the country, detection of a material weakness or identification of attack tools that constitute a direct threat to the licensee.**

OM-7.1 General Requirements

OM-7.1.1 **The requirements in Section OM-7.1 apply to Bahraini Islamic bank licensees, with respect to the business activities of the whole bank (whether booked in Bahrain or in a foreign branch). The requirements in Section OM-7.1 also apply to overseas Islamic bank licensees, but only with respect to the business booked in their branch in Bahrain.**

OM-7.1.2 **With reference to Articles 59 and 60 of the CBB Law, all Islamic bank licensees must maintain books and records (whether in electronic or hard copy form) sufficient to produce financial statements and show a complete record of the business undertaken by a licensee. These records must be retained for at least 10 years according to Article 60 of the CBB Law.**

OM-7.1.3 OM-7.1.2 includes accounts, books, files and other records (e.g. trial balance, general ledger, nostro/vostro statements, reconciliations and list of counterparties). It also includes records that substantiate the value of the assets, liabilities and off-balance sheet activities of the licensee (e.g. client activity files and valuation documentation).

OM -7.1.4 [This Paragraph was deleted in April 2011]

OM-7.1.5 **Unless otherwise agreed with the CBB in writing, records must be kept in either English or Arabic; or else accompanied by a certified English or Arabic translation. Records must be kept current. The records must be sufficient to allow an audit of the licensee's business or an on-site examination of the licensee by the CBB.**

OM -7.1.6 If a licensee wishes to retain certain records in a language other than English or Arabic without translation, the licensee should write to the CBB, explaining which types of records it wishes to keep in a foreign language, and why systematically translating these may be unreasonable. Generally, only loan contracts or similar original transaction documents may be kept without translation. Where exemptions are granted by CBB, the licensee is nonetheless asked to confirm that it will make available certified translations of such documents, if requested by CBB for an inspection or other supervisory purpose.

OM -7.1.7 Translations produced in compliance with Rule OM-7.1.5 may be undertaken in-house, by an employee or contractor of the licensee, provided they are certified by an appropriate officer of the licensee.

OM-7.1 General Requirements (continued)

OM-7.1.8 **Records must be accessible at any time from within the Kingdom of Bahrain, or as otherwise agreed with the CBB in writing.**

OM-7.1.9 Where older records have been archived, or in the case of records relating to overseas branches of Bahraini Islamic banks, the CBB may accept that records be accessible within a reasonably short time frame (e.g. within 5 business days), instead of immediately. The CBB may also agree similar arrangements for overseas Islamic banks, as well as Bahraini Islamic banks, where elements of record retention and management have been centralised in another group company, whether inside or outside of Bahrain.

OM-7.1.10 All original account opening documentation, due diligence and transaction documentation should normally be kept in Bahrain, if the business is booked in Bahrain. However, where a licensee books a transaction in Bahrain, but the transaction documentation is handled entirely by another (overseas) branch or affiliate of the licensee, the relevant transaction documentation may be held in the foreign office, provided electronic or hard copies are retained in Bahrain; the foreign office is located in a FATF member state; and the foreign office undertakes to provide the original documents should they be required.

OM-7.1.11 Licensees should also note that to perform effective consolidated supervision of a group (or sub-group), the CBB needs to have access to financial information from foreign operations of a licensee, in order to gain a full picture of the financial condition of the group: see Module BR (CBB Reporting), regarding the submission of consolidated financial data. If a licensee is not able to provide to the CBB full financial information on the activities of its branches and subsidiaries, it should notify the CBB of the fact, to agree alternative arrangements: these may include requiring the group to restructure or limit its operations in the jurisdiction concerned.

OM-7.1.12 **In the case of Bahraini Islamic banks with branch operations overseas, where local record-keeping requirements are different, the higher of the local requirements or those contained in this Chapter must be followed.**

OM-7.2 Transaction Records

OM-7.2.1 **Islamic bank licensees must keep completed transaction records for as long as they are relevant for the purposes for which they were made (with a minimum period in all cases of five years from the date when the transaction was completed – see Module Section FC-7.1). Records of completed transactions must be kept whether in hard copy or electronic format, for at least five years from the date of the transaction as per the Legislative Decree No. (28) of 2002 with respect to Electronic Transactions "The Electronic Transaction Law" and its amendments.**

OM-7.2.2 [This paragraph has been deleted in July 2017].

OM-7.2.3 **Rule OM-7.2.1 applies to all transactions entered into by a Bahraini Islamic bank licensee, whether booked in Bahrain or in an overseas branch. With respect to overseas Islamic bank licensees, it applies only to transactions booked in the Bahrain branch.**

OM-7.2.4 In the case of overseas Islamic bank licensees, Rule OM-7.2.1 therefore only applies to business booked in the Bahrain branch, not in the rest of the company.

OM-7.3 Other Records

Corporate Records

OM-7.3.1 **Islamic bank licensees must maintain the following records in original form or in hard copy at their premises in Bahrain:**

(a) Internal policies, procedures and operating manuals;

(b) Corporate records, including minutes of shareholders', Directors' and management meetings;

(c) Correspondence with the CBB and records relevant to monitoring compliance with CBB requirements;

(d) Reports prepared by the Islamic bank licensee's internal and external auditors; and

(e) Employee training manuals and records.

OM-7.3.2 In the case of Bahrain Islamic bank licensees, these requirements apply to the licensee as a whole, including any overseas branches. In the case of overseas Islamic bank licensees, all the requirements of Chapter OM-7 are limited to the business booked in their branch in Bahrain and the records of that branch (see Rule OM-7.1.1). They are thus not required to hold copies of shareholders' and Directors' meetings, except where relevant to the branch's operations.

Customer Records

OM-7.3.3 Record-keeping requirements with respect to customer records, including customer identification and due diligence records, are contained in Module FC (Financial Crime). These requirements address specific requirements under the Amiri Decree Law No. 4 of 2001, the standards promulgated by the Financial Action Task Force, as well as to the best practice requirements of the Basel Committee Core Principles methodology, and its paper on "Customer due diligence for banks".

Promotional Schemes

OM-7.3.4 **Islamic bank licensees must maintain all material related to promotional schemes as outlined in Section BC-1.1 for a minimum period of 5 years.**

OM-8.1 [This Chapter was deleted in March 2019 and requirements are now covered under Chapter OM-2.] ~~Introduction~~

~~OM-8.1.1 The contents of this Chapter apply in full to all Bahraini Islamic bank licensees both on a consolidated basis and on a solo basis.~~

~~OM-8.1.1A This Chapter may be used as guidance for overseas Islamic bank licensees.~~

~~OM-8.1.1.B Section CA-6.2 of the Capital Adequacy Module allows banks to use either the basic indicator approach or standardised approach to compute capital charge for operational risk. This chapter sets out the qualitative aspect of these two approaches.~~

~~OM-8.1.2 Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events which includes but is not limited to, legal risk[1] and Shariah compliance risk. This definition excludes strategic and reputational risk.~~

~~OM-8.1.3 Operational risk is inherent in all banking products, activities, processes and systems, and the effective management of operational risk must be a fundamental element of a bank's risk management programme. Sound operational risk governance relies upon three lines of defence:~~

~~(a) Business line management;~~
~~(b) An independent operational risk management function; and~~
~~(c) Independent review functions.~~

~~OM-8.1.4 In the context of this Chapter, 'independent' and 'independent review' have the following meanings. The review functions must be independent of the risk generating business lines or the process or system under review. An independent review would include the following components:~~

~~(a) Verification of the Framework is done on a periodic basis and would be typically performed by the bank's internal and/or external audit, but may involve other suitably qualified independent parties from external sources. Verification activities test the effectiveness of the overall Framework, consistent with policies approved by the board of directors, and also test validation processes to ensure that they are independent and implemented in a manner consistent with established bank policies; and~~

~~(b) Validation ensures that the quantification systems used by the bank are sufficiently robust and provide assurance of the integrity of inputs, assumptions, processes and outputs. Specifically the independent validation process should provide enhanced assurance that the risk management methodology results in an operational risk capital charge that credibly reflects the operational risk profile of the bank. In addition to the quantitative aspects of internal validation, the validation of data inputs, methodology and outputs of operational risk models is important to the overall process.~~

~~[1] Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.~~

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.1 Introduction (continued)

OM-8.1.5 The operational risk management function must be functionally independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk Framework ("Framework" – see also Paragraphs OM-8.2.12 and OM-8.2.13 for a description of the "Framework") within the bank.

OM-8.1.6 For the purpose of Paragraph OM-8.1.5, "functionally independent" means that the risk management function cannot report hierarchically and/or functionally to any person or function that is directly responsible for risk generation.

OM-8.1.7 The operational risk management function should include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the operational risk management function is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems. The operational risk management function should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.

OM-8.1.8 The independent review functions are the audit and compliance functions and the staff occupying these functions must be competent and appropriately trained and not be involved in the development, implementation and operation of the operational risk Framework (for example, internal audit and compliance must not be involved with the setting of risk appetite or risk tolerance, but internal audit should be reviewing the robustness of the process of how these limits are set and why and how they are adjusted in response to changing circumstances). Internal Audit should independently verify that the Framework has been implemented as intended and is functioning effectively. Internal audit coverage should include opining on the overall appropriateness and adequacy of the Framework and the associated governance processes across the bank. Internal audit should not simply be testing for compliance with board approved policies and procedures, but should be evaluating whether the Framework meets organisational needs and supervisory expectations. More details on the Internal Audit Function and the Role of the Audit Committee are to be found in Chapter HC-3.

OM-8.2 [This Chapter was deleted in March 2019 and requirements are now covered under Chapter OM-2.]~~Basic Indicator Approach~~

~~OM-8.2.1 Banks applying the basic indicator approach for capital adequacy purposes as detailed in Section CA-6.2 of Module CA (Capital Adequacy) are encouraged to comply with the principles set forth in this Section.~~

~~Fundamental Principles of Operational Risk Management~~

~~OM-8.2.2 Principle 1: The board of directors must take the lead in establishing a strong risk management culture. The board of directors and senior management must establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.~~

~~OM-8.2.3 Banks with a strong culture of risk management and ethical business practices are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with those events that do occur. The actions of the board and senior management, and policies, processes and systems provide the foundation for a sound risk management culture. More details on the role of the board and senior management are to be found in Chapters HC-1, HC-2, and HC-6 as well as in Chapters CM-1 and OM-2.~~

~~OM-8.2.4 The board must establish a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts (see Section HC-2.2).~~

~~OM-8.2.5 Clear expectations and accountabilities ensure that bank staff understand their roles and responsibilities for risk, as well as their authority to act. Strong and consistent senior management support for risk management and ethical behaviour convincingly reinforces codes of conduct and ethics, compensation strategies, and training programmes.~~

~~OM-8.2.6 Compensation policies must be aligned to the bank's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They must also appropriately balance risk and reward (see Chapter HC-5 concerning remuneration).~~

~~OM-8.2.7 Banks should refer to the Financial Stability Board's Principles for Sound Compensation Practices, published in September 2009 regarding compensation policies.~~

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.8 Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organisation. Training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.

OM-8.2.9 Principle 2: Banks must develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

OM-8.2.10 The fundamental premise of sound risk management is that the board of directors and bank management understand the nature and complexity of the risks inherent in the portfolio of bank 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.

OM-8.2.11 A vital means of understanding the nature and complexity of operational risk is to have the components of the Framework fully integrated into the overall risk management processes of the bank. The Framework should be appropriately integrated into the risk management processes across all levels of the organisation including those at the group and business line levels, as well as into new business initiatives' products, activities, processes and systems. In addition, results of the bank's operational risk assessment should be incorporated into the overall bank business strategy development processes.

OM-8.2.12 The Framework must be comprehensively and appropriately documented in board of directors approved policies and must include definitions of operational risk and operational loss. Banks that do not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of their Framework.

OM-8.2.13 Framework documentation must clearly:

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

(b) Describe the risk assessment tools and how they are used;

(c) Describe the bank's accepted operational risk appetite and tolerance (see Paragraphs OM-8.2.17 and OM-8.2.18), as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;

(d) Describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

(e) Establish risk reporting and Management Information Systems (MIS);

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

(f) Provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives;

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

(h) Require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate.

Governance: The Board of Directors

OM-8.2.14 Principle 3: The board of directors must establish, approve and periodically review the Framework. The board of directors must oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

OM-8.2.15 The board of directors must:

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

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

(c) Regularly review the Framework to ensure that the bank has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes or systems, including changes in risk profiles and priorities (e.g. changing business volumes);

(d) Ensure that the bank's Framework is subject to effective independent review by audit or other appropriately trained parties such as the compliance function; and

(e) Ensure that as best practice evolves, management is availing themselves of these advances.

OM-8.2.16 Strong internal controls are a critical aspect of operational risk management, and the board of directors must establish clear lines of management responsibility and accountability for implementing a strong control environment. The control environment must provide appropriate independence/separation of duties between operational risk management functions, business lines and support functions.

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.17 Principle 4: The board of directors must approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume.

OM-8.2.18 When approving and reviewing the risk appetite and tolerance statement, the board of directors must consider all relevant risks, the bank's level of risk aversion, its current financial condition and the bank's strategic direction. The risk appetite and tolerance statement should encapsulate the various operational risk appetites within a bank and ensure that they are consistent. The board of directors must approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite and tolerance.

OM-8.2.19 The board of directors must regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statement. This review must consider changes in the external environment, material 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 or nature of limit breaches. The board must monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.

Senior Management

OM-8.2.20 Principle 5: Senior management must develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.21 Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. These must include systems to report, track and, when necessary, escalate issues to ensure resolution. Banks must be able to demonstrate that the three lines of defence (as highlighted in Paragraph OM-8.1.3) approach is operating satisfactorily and to explain how the board and senior management ensure that this approach is implemented and operating in an appropriate and acceptable manner.

OM-8.2.22 Senior management must translate the operational risk management Framework established by the board of directors into specific policies, processes and procedures that can be implemented and verified within the different business units. Senior management must clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability, and ensure that the necessary resources are available to manage operational risk in line with the bank's risk appetite and tolerance statement. Moreover, senior management must ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.

OM-8.2.23 Senior management must ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as insurance risk transfer and outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

OM-8.2.24 A bank's risk management function should be commensurate with the nature, size, complexity and risk profile of the bank's activities. The managers of the corporate operational risk management function should be of sufficient stature within the bank to perform their duties effectively, ideally evidenced by title commensurate with other risk management functions such as credit, market and liquidity risk.

OM-8.2.25 Senior management should ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should have authority independent from the units they oversee.

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.26 **A bank's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, a bank must take the following into consideration:**
(a) Committee structure;
(b) Committee composition; and
(c) Committee operation.

OM-8.2.27 Sound industry practice for larger and more complex organisations with a central group function and separate business units is to utilise a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from operational risk committees by country, business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board's risk management committee.

OM-8.2.28 Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include a combination of members with expertise in business activities and financial, as well as independent risk management (refer to Module HC for details on committee membership).

OM-8.2.29 Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

Risk Management Environment: Identification and Assessment

OM-8.2.30 **Principle 6: Senior management must ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.**

OM-8.2.31 Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal factors (such as the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes and employee turnover) and external factors (such as changes in the broader environment and the industry and advances in technology). Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively.

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.32 Examples of tools that may be used for identifying and assessing operational risk include:

(a) Audit Findings: While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors;

(b) Internal Loss Data Collection and Analysis: Internal operational loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic. Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure;

(c) 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 organisations other than the bank. 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;

(d) Risk Assessments: In a risk assessment, often referred to as a Risk Self Assessment (RSA), a bank 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 Assessments (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 the RCSA output into metrics that give a relative ranking of the control environment;

(e) Business Process Mapping: Business process mappings identify the key steps in business processes, activities and organisational functions. They also 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. They also can help prioritise subsequent management action;

(f) Risk and Performance Indicators: Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank's risk exposure. Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks. Performance indicators, often referred to as Key Performance Indicators (KPIs), 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;

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

(g) Scenario Analysis: Scenario analysis is a process of obtaining expert opinion of 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. Given the subjectivity of the scenario process, a robust governance Framework is essential to ensure the integrity and consistency of the process;

(h) Measurement: Larger banks 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 of the model can be used in an economic capital process and can be allocated to business lines to link risk and return; and

(i) Comparative Analysis: Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank's operational risk profile. For example, comparison of the frequency and severity of internal data with RCSAs can help the bank 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 bank's exposure to potential risk events.

OM-8.2.33 The bank must ensure that the internal pricing and performance measurement mechanisms appropriately take into account operational risk. Where operational risk is not considered, risk-taking incentives might not be appropriately aligned with the risk appetite and tolerance.

OM-8.2.34 Principle 7: Senior management must ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

OM-8.2.35 In general, a bank's operational risk exposure is increased when a bank engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Moreover, the level of risk may escalate when new products activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business-critical operations. A bank should 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.

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.36 A bank 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 should consider:
(a) Inherent risks in the new product, service, or activity;
(b) Changes to the bank'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 or activity.

OM-8.2.37 The approval process should also include ensuring that appropriate investment has been made for human resources and technology infrastructure before new products are introduced. The implementation of new products, activities, processes and systems should be monitored in order to identify any material differences to the expected operational risk profile, and to manage any unexpected risks.

Monitoring and Reporting

OM-8.2.38 Principle 8: Senior management must implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms must be in place at the board, senior management, and business line levels that support proactive management of operational risk.

OM-8.2.39 Banks are encouraged to continuously improve the quality of operational risk reporting. A bank should ensure that its reports are comprehensive, accurate, consistent and actionable across business lines and products. Reports should be manageable in scope and volume; effective decision-making is impeded by both excessive amounts and paucity of data.

OM-8.2.40 Reporting should be timely and a bank should be able to produce reports in both normal and stressed market conditions. The frequency of reporting should reflect the risks involved and the pace and nature of changes in the operating environment. The results of these monitoring activities should be included in regular management and board reports, as should assessments of Framework performed by the internal audit and/or risk management and compliance functions. Reports generated by (and/or for) supervisory authorities should also be reported internally to senior management and the board, where appropriate.

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.41 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. Operational risk reports should include:

(a) Breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits;

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

(c) Relevant external events and any potential impact on the bank and operational risk capital.

OM-8.2.42 Data capture and risk reporting processes should be analysed periodically with a view to continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.

Control and Mitigation

OM-8.2.43 Principle 9: Banks must have a strong control environment that utilises:

(a) Policies, processes and systems;

(b) Appropriate internal controls; and

(c) Appropriate risk mitigation and/or transfer strategies.

OM-8.2.44 Internal controls must be designed to provide assurance that a bank will:

(a) Have efficient and effective operations;

(b) Safeguard its assets;

(c) Produce reliable financial reports; and

(d) Comply with applicable laws and regulations.

OM-8.2.45 A sound internal control programme consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities. These components are outlined in more detail in the Basel Committee paper "Framework for Internal Control Systems in Banking Organisations".

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.46 Control processes and procedures should be established and banks should have a system in place for ensuring compliance with a documented set of internal policies concerning the risk management system. Principal elements of this could include, for example:

(a) Top-level reviews of the bank's progress towards the stated objectives;
(b) Verifying compliance with management controls;
(c) Review of the treatment and resolution of instances of non-compliance;
(d) Evaluation of required approvals and authorisations to ensure accountability to an appropriate level of management; and
(e) Tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy.

OM-8.2.47 An effective internal control environment also requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals, or a team without dual controls or other countermeasures may enable concealment of losses, errors or inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimised, and subject to careful independent monitoring and review.

OM-8.2.48 In addition to segregation of duties and dual controls, banks should ensure that other traditional internal controls are in place as appropriate to address operational risk. Examples of these controls include:

(a) Clearly established authorities and/or processes for approval;
(b) Close monitoring of adherence to assigned risk limits or thresholds;
(c) Safeguards for access to, and use of, bank assets and records;
(d) Appropriate staffing level and training to maintain expertise;
(e) Ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;
(f) Regular verification and reconciliation of transactions and accounts; and
(g) A vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.

OM-8.2.49 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 programmes.

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.50 The use of technology-related products, activities, processes and delivery channels exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks. Sound technology risk management uses the same precepts as operational risk management and includes:

(a) Governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives;

(b) Policies and procedures that facilitate identification and assessment of risk;

(c) Establishment of a risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk;

(d) Implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and

(e) Monitoring processes that test for compliance with policy thresholds or limits.

OM-8.2.51 Management should ensure the bank has a sound technology infrastructure that:

(a) Meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress;

(b) Ensures data and system integrity, security, and availability; and

(c) Supports integrated and comprehensive risk management.

OM-8.2.52 Mergers and acquisitions resulting in fragmented and disconnected infrastructure, cost-cutting measures or inadequate investment can undermine a bank'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, or oversee and manage risk in periods of high growth. 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.

OM-8.2.53 In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party such as through insurance. The board of directors should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should perform an annual review of the bank's risk and insurance management programme.

MODULE	OM: Operational Risk Management
CHAPTER	OM-8: Qualitative Aspects

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.54 Because risk transfer is an imperfect substitute for sound controls and risk management programmes, banks should view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place 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 insurance truly reduce risk, transfer the risk to another business sector or area, or create a new risk (e.g. counterparty risk).

Role of Disclosure

OM-8.2.55 Principle 10: A bank's public disclosures must allow stakeholders to assess its approach to operational risk management.

OM-8.2.56 A bank's public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations, and evolving industry practice. See also Chapter HC-8 and Chapter PD-1 on disclosure requirements.

OM-8.2.57 A bank should disclose its operational risk management Framework in a manner that will allow stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively.

OM-8.2.58 A bank's disclosures should be consistent with how senior management and the board of directors assess and manage the operational risk of the bank.

OM-8.2.59 A bank must have a formal disclosure policy approved by the board of directors that addresses the bank's approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, banks must implement a process for assessing the appropriateness of their disclosures, including the verification and frequency of them.

OM-8.3 Standardised Approach

OM-8.3.1 **Banks applying standardised approach for capital adequacy purposes as detailed in section CA-6.2 of Capital Adequacy Module, must satisfy the principles set out in section OM-8.2 and in this Section. In order to qualify for use of the Standardised Approach, a bank must satisfy the CBB that, at a minimum:**

(a) Its board of directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework (see principles 1-3);

(b) It has an operational risk management system that is conceptually sound and is implemented with integrity (see principles 4-7); and

(c) It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.

OM-8.3.2 The CBB will have the right to insist on a period of initial monitoring of a bank's Standardised Approach before it is used for regulatory capital purposes.

OM-8.3.3 **A bank must develop specific policies and have documented criteria for mapping gross income for current business lines and activities into the standardised framework. The criteria must be reviewed and adjusted for new or changing business activities as appropriate. Further guidance on business line mapping is set out in paragraph CA-6.2.8 of the Capital Adequacy Module.**

OM-8.3.4 **A bank using the standardised approach must meet the following additional criteria:**

(a) The bank must have an operational risk management system with clear responsibilities assigned to an operational risk management function. The operational risk management function is responsible for developing strategies to identify, assess, monitor and control/mitigate operational risk; for codifying bank-level policies and procedures concerning operational risk management and controls; for the design and implementation of the bank's operational risk assessment methodology; and for the design and implementation of a risk-reporting system for operational risk;

OM-8.3 Standardised Approach (continued)

(b) As part of the bank's internal operational risk assessment system, the bank must systematically track relevant operational risk data including material losses by business line. Its operational risk assessment system must be closely integrated into the risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the banks operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, and risk analysis. The bank must have techniques for creating incentives to improve the management of operational risk throughout the bank;

(c) There must be regular reporting of operational risk exposures, including material operational losses, to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports;

(d) [This subparagraph was deleted in October 2012];

(e) [This subparagraph was deleted in October 2012]; and

(f) The bank's operational risk assessment system (including the internal validation processes) must be subject to regular review by external auditors and /or the CBB.

MODULE	OM: Operational Risk Management
CHAPTER	Appendix A: Loss Event Type Classification

Appendix A

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Internal Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party.	Unauthorised Activity	• Transactions not reported (intentional) • Transaction type unauthorised (w/monetary loss) • Mismarking of position (intentional)
		Theft and Fraud	• Fraud/credit fraud/worthless deposits • Theft/extortion/embezzlement/robbery • Misappropriation of assets • Malicious destruction of assets, forgery, check kiting and smuggling • Account take-over/impersonation/etc. • Tax non-compliance/evasion (wilful) • Bribes/kickbacks • Insider trading (not on
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.	Theft and Fraud	• Theft/robbery • Forgery and check kiting
		Systems Security	• Hacking damage • Theft of information (w/monetary loss)
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.	Employee Relations	• Compensation, benefit, termination issues • Organised labour activity
		Safe Environment	• General liability (slip and fall, etc.) • Employee health & safety rules events • Workers compensation
		Diversity and Discrimination	• All discrimination types

Appendix A (Continued)

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Clients, Products and Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, Disclosure and Fiduciary	• Fiduciary breaches/ guideline violations • Suitability/disclosure issues (KYC, etc.) • Retail customer disclosure violations • Breach of privacy • Aggressive sales • Account churning • Misuse of confidential information • Lender liability
		Improper Business or Market Practices	• Antitrust • Improper trade/market practices • Market manipulation • Insider trading (on firm's account) • Unlicensed activity • Money laundering
		Product Flaws	• Product defects (unauthorised, etc.) • Model errors
		Selection, Sponsorship and Exposure	• Failure to investigate client per guidelines • Exceeding client exposure limits
		Advisory Activities	• Disputes over performance of advisory activities
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Disasters and other events	• Natural disaster losses • Human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures.	Systems	• Hardware • Software • Telecommunications • Utility outage/disruptions

Appendix A (Continued)

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Execution, Delivery and Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.	Transaction Capture, Execution and Maintenance	• Miscommunication • Data entry, maintenance or loading error • Missed deadline or responsibility • Model/system misoperation • Accounting error/entity attribution error • Other task misperformance • Delivery failure • Collateral management failure • Reference data
		Monitoring and Reporting	• Failed mandatory reporting obligation • Inaccurate external report (loss incurred)
		Customer Intake and Documentation	• Client permissions/disclaimers missing • Legal documents
		Customer/Client Account Management	• Unapproved access given to accounts • Incorrect client records (loss incurred) • Negligent loss or damage of client assets
		Trade Counterparties	• Non-client counterparty misperformance • Misc. non-client counterparty disputes
		Vendors and Suppliers	• Outsourcing • Vendor disputes

Appendix ~~OM-1~~B

Set out below are examples of Shariah requirements that are to be complied with by the banks in respect of the financing contracts. The list is for guidance purposes and not conclusive and may vary according to the views of the various Shariah Supervisory Board (SSB):

(a) Murabahah and Ijarah contracts

- The asset is in existence at the time of sale or lease or, in case of Ijarah, the lease contract should be preceded by acquisition of the usufruct of the asset except if the asset was agreed upon based on a general specification.
- The asset is legally owned by the bank when it is offered for sale.
- The asset is intended to be used by the buyer/ lessee for activities or businesses permissible by Shariah; if the asset is leased back to its owner in the first lease period, it should not lead to contract of 'inah, by varying the rent or the duration.
- 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 debtor is solvent or insolvent.

(b) Salam and Istisna' contracts

- A sale and purchase contract cannot be inter-dependent and inter-conditional on each other, such as Salam and Parallel Salam; Istisna' and Parallel Istisna'.
- It is not allowed to stipulate a penalty clause in respect of delay in delivery of a commodity that is purchased under Salam contract, however it is allowed under Istisna' or Parallel Istisna'.
- The subject-matter of an Istisna' contract may not physically exist upon entering into the contract.

(c) Musharakah and Mudarabah contracts

- The capital of the bank is to be invested in Shariah compliant investments or business activities.
- A partner in Musharakah cannot guarantee the capital of another partner or a Midrib guarantees the capital of the Mudarabah.
- The purchase price of other partner's share in a Musharakah with a binding promise to purchase can only be set as per the market value or as per the agreement at the date of buying. It is not permissible, however, to stipulate that the share be acquired at its face value.