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;
(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 Module History

OM-A.2.1 This Module was first issued in July 2004 as part of Volume two of the CBB Rulebook. Any 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.2.2 The 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 2.
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.2 Module History (continued)

OM-A.2.3 (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.2 Module History (continued)

OM-A.2.3 (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.
OM Module	01/2020	Entire Module revised for better alignment with the principles and guidance from Basel Committee on Banking Supervision.
OM-5.2.1A	07/2020	Added a new Paragraph on contactless payments.
OM-5.1.2A & OM-5.1.2B	10/2020	Added new Paragraphs on fraudulent phishing attempts measures.
OM-2.8.5	01/2021	Deleted Subparagraph (a).
OM-3.1.2(f)	01/2021	Amended Subparagraph on electronic fraud.
OM-3.3.11	01/2021	Added a new Paragraph on electronic fraud awareness.
OM-5.1.5	04/2021	Amended Paragraph.
OM-5.5	07/2021	New enhanced Section.
Appendix C	07/2021	Added a new Appendix - Cyber security Control Guidelines.
OM-1.6.1	01/2022	Deleted Paragraph.
OM-1.6.2	01/2022	Deleted Paragraph.
OM-1.6.3	01/2022	Amended Paragraph.
OM-1.6.4 – OM-1.6.6	01/2022	Deleted Paragraphs.
OM-5.3.2	01/2022	Amended Paragraph.
OM-5.3.3 – OM-5.3.11	01/2022	Deleted Paragraphs.
OM-1.3.17(g)	04/2022	Amended Subparagraph on vacation policy.
OM-5.5.57	04/2022	Amended Paragraph on cyber security incident reporting.
OM-5.5.58	04/2022	Amended Paragraph on submission period of the cyber security incident report.
OM-5.5.61	04/2022	Deleted reference to BR.
OM-2	07/2022	Replaced Chapter OM-2 with new Outsourcing Requirements.
OM-5.3.25	10/2022	Added a new Paragraph on compliance with the physical security requirements for ATM installations.
OM-5.5.21	10/2022	Amended Paragraph on email domains requirements.
OM-5.5.21A	10/2022	Added a new Paragraph on additional domains requirements.
OM-2.1.7(v)	04/2023	Amended Subparagraph on the outsourcing coordinator.
OM-2.1.7(viii)	04/2023	Added a new Subparagraph on outsourcing the internal audit function.
OM-5.2.1 – OM-5.2.1A	04/2023	Amended contactless payment amount permitted where no pin or authentication is required.

OM-B.1 Scope of Application

Bahraini Islamic Bank Licensees

OM-B.1.1 **Bahraini Islamic bank licensees must comply with all requirements included in this Module.**

OM-B.1.2 The Framework for operational risk management and the structure of governance process for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

Branches of foreign bank licensees

OM-B.1.3 In the case of branches of foreign bank licensees, while the requirements of this Module apply, it is recognised that certain activities and tasks relating to operational risk management function or unit might be conducted at the head office or a regional office. Additionally, in the case of branches, it is likely that oversight of the branch, from an operational risk perspective, is also exercised at the head office/regional office.

OM-B.1.4 **Branches of foreign bank licensees must document the risk assessments which, at a minimum, include the identified risk events by risk type or category, the key risk indicators (KRIs) and key control indicators (KCIs). In addition, the branch must record losses arising from failures of people, processes, systems, internal and external frauds.**

OM-B.1.5 **Branches of foreign bank licensees must seek the CBB's approval for the operational risk management activities undertaken by their head/regional office and demonstrate to the CBB that there are effective high-level controls for management of operational risk for activities undertaken out of the Bahrain branch.**

OM-B.1.6 For the purposes of such CBB approval, the branch must perform a mapping or a gap analysis of the requirements in this Module with practices undertaken at the head office or regional office, whichever applicable, and at the branch as appropriate.

MODULE	OM: Operational Risk Management
CHAPTER	OM-1: General Requirements

OM-1.1 Operational Risk Management Framework

Overview

OM-1.1.1 This chapter contains the requirements relating to operational risk management. It sets out the requirements for an appropriate risk management environment. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems including internal frauds, or from external events including 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 requirements included in this Module are also applied to the management of legal risks requirement.

OM-1.1.2 Operational risk is inherent in all types of bank activities and can result in substantial losses. 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 functions that provide independent assurance.

OM-1.1.3 **All new products and services must 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 risk in the scope of internal audits.**

OM-1.1.4 Shari'a non-compliance is a unique risk for Islamic banks resulting from non-compliance with the rules and principles of Shari'a. It is crucial to identify 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.

OM-1.1 Operational Risk Management Framework (Continued)

Establishing a Strong Risk Culture

OM-1.1.5 **The Board of Directors must take the lead in establishing a strong operational risk management culture in the bank that supports and provides appropriate standards and incentives for effectively managing operational risk and for promoting professional and responsible behaviour.**

OM-1.1.6 For branches of foreign bank licensees, all references in this Module to the board of directors should be interpreted as the Head Office/ Regional Office unless such responsibility is formally delegated to a committee at the branch level.

Operational Risk Management Framework

OM-1.1.7 **Islamic bank licensees 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-1.1.8 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-1.1.9 **A bank must ensure that its ORMF 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.**

OM-1.1 Operational Risk Management Framework (Continued)

OM-1.1.10 At minimum, the ORMF documentation must:

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

(b) Identify policy for approval of policies by the Board;

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

(d) Describe the bank's accepted operational risk appetite and tolerance (see Paragraphs OM-1.2.2 to OM-1.2.4), and the approach to setting thresholds or limits for inherent and residual risk, and approved risk mitigation strategies;

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

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

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

OM-1.2 Operational Risk Governance

OM-1.2.1 **The Board of Directors must:**

(a) Establish, approve and regularly review the operational risk management policy;

(b) Ensure that senior management establish, approve and regularly review supporting policies, procedures, systems and processes in line with the nature and scope of the operational risks inherent in the bank's products, services and activities, and implement comprehensive, dynamic oversight and control environments that are fully integrated into, or coordinated with, the overall ORMF for managing all risks across the bank; and

(c) Ensure that the bank's ORMF is subject to effective independent review (See Paragraph OM-1.6.1).

Risk appetite

OM-1.2.2 **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-1.2.3 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-1.2.4 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 and mitigation strategies, loss experience, and the frequency, volume and nature of limit breaches.

OM-1.2.5 **The board must monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.**

OM-1.2 Operational Risk Governance (Continued)

OM-1.2.6 **Senior management is responsible for consistently implementing and maintaining throughout the organisation, the policy, procedures, processes and systems for managing operational risk in all of the bank's products, activities, processes and systems.**

OM-1.2.7 **Banks must establish, commensurate with its nature, size and complexity, an Operational Risk Management Unit (ORMU), independent of the risk generating business lines, which is responsible for the design, maintenance and ongoing development of the ORMF within the bank. The ORMU must be adequately staffed with skilled resources.**

OM-1.2.8 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-1.1.2) 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-1.2.9 **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-1.2.10 Senior management should ensure that staff responsible for managing operational risk, coordinate and communicate effectively with staff responsible for managing credit, market, liquidity 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-1.2 Operational Risk Governance (Continued)

OM-1.2.11 **The Head of the ORMU 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-1.2.12 **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 policies must be independent from the units they oversee.**

OM-1.2.13 **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-1.2.14 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-1.2.15 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-1.2.16 Committee meetings should be held at appropriate frequencies, with adequate time and resources to permit productive discussion and decision-making. Records of committee meetings should be adequate to permit review and evaluation of committee effectiveness.

OM-1.3 Identification, Measurement, Monitoring and Control

OM-1.3.1 **As part of an effective ORMF, banks must have policies, procedures and system for the identification, measurement, monitoring, mitigating and controlling of the operational risk inherent in all products, services, activities, processes and systems.**

OM-1.3.2 Risk identification and assessment are fundamental characteristics of an effective ORMF. 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 may use the classification categories contained in Appendix A for determining and classifying operational risk events.

OM-1.3.3 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;

OM-1.3 Identification, Measurement, Monitoring and Control (Continued)

(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;

(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-1.3.4 Banks should ensure that the internal pricing and performance measurement mechanisms appropriately take into account operational risk measures commensurate with the nature, size and complexity of its business operations.

OM-1.3 Identification, Measurement, Monitoring and Control (Continued)

New Products, Process and Change Management

OM-1.3.5 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-1.3.6 **A bank must have a policy and procedures for review and approval of new products, services, activities, procedures, processes and systems. The review and approval process must consider, as appropriate, the following:**

(a) Inherent and residual risks;
(b) Changes to the bank's operational risk profile and appetite and tolerance;
(c) The necessary controls, risk management processes and risk mitigation strategies;
(d) Changes to relevant risk thresholds or limits; and
(e) The procedures and metrics to measure, monitor, and manage the risk.

OM-1.3.7 **The approval process must also ensure that adequate and well-trained human resources and appropriate technology infrastructure are in place before new products, services, activities, procedures, processes 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.**

OM-1.3 Identification, Measurement, Monitoring and Control (Continued)

OM-1.3.8 The use of technology-related products, services, 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-1.3.9 **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-1.3.10 **Banks must ensure that the operational risk reports are comprehensive, accurate, consistent and actionable across business lines and products.**

OM-1.3.11 **Reporting should be timely, and the 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. Reports generated by (and/or for) supervisory authorities must also be reported internally to senior management and the Board, where appropriate.**

OM-1.3.12 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-1.3 Identification, Measurement, Monitoring and Control (Continued)

OM-1.3.13 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-1.3.14 **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-1.3.15 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-1.3.16 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-1.3.17 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 in line with Bahrain Labour Law.

OM-1.3 Identification, Measurement, Monitoring and Control (Continued)

OM-1.3.18 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-1.3 Identification, Measurement, Monitoring and Control (Continued)

OM-1.3.19 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-1.3.20 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-1.3.21 **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-1.3.22 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-1.3.23 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.

OM-1.3 Identification, Measurement, Monitoring and Control (Continued)

OM-1.3.24 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).

OM-1.4 Succession Planning

OM-1.4.1 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-1.4.2 **The CBB requires Islamic bank licensees to document their Board-approved succession plans for their senior management team and have these ready at any time for onsite inspection by CBB.**

OM-1.5 Public Disclosure

OM-1.5.1 **A bank must have a formal disclosure policy approved by the Board of Directors that addresses the bank's approach for determining what operational risks 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-1.5.2 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-1.5.3 **A bank must 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-1.5.4 **A bank's disclosures must be consistent with how senior management and the Board of Directors assess and manage the operational risks of the bank.**

OM-1.6 Independent Review

OM-1.6.1 **[This Paragraph was deleted in January 2022].**

OM-1.6.2 [This Paragraph was deleted in January 2022].

OM-1.6.3 **The independent review of the operational risk management framework undertaken in accordance with Paragraphs HC-6.6.33 and HC-6.6.34, must cover the following:**

(i) Governance, the role of the board and senior management and ORMU in operational risk management;

(ii) The existence of operational risk appetite/tolerances or thresholds and approved documented policies, procedures and processes including tools for risk identification and assessment;

(iii) Register of risks covering risk events, KRIs, KRDs, KCIs and risk mitigation techniques;

(iv) Policies to ensure the bank are in compliance with the requirements under this Module for outsourcing arrangements including cloud outsourcing, electronic banking, security arrangements and business continuity management.

OM-1.6.4 [This Paragraph was deleted in January 2022].

OM-1.6.5 **[This Paragraph was deleted in January 2022].**

OM-1.6.6 **[This Paragraph was deleted in January 2022].**

OM-2.1 Outsourcing Arrangements

OM-2.1.1 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-2.1.2 In the context of this Chapter, 'outsourcing' means an arrangement whereby a third party performs on behalf of a licensee an activity which 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-2.1.3 In the case of branches of foreign entities, the CBB may consider a third-party outsourcing arrangement entered into by the licensee's head office/regional office or other offices of the foreign entity as an intragroup outsourcing, provided that the head office/regional office submits to the CBB a letter of comfort which includes, but is not limited to, the following conditions:

i. The head office/regional office declares its ultimate responsibility of ensuring that adequate control measures are in place; and
ii. The head office/regional 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.

OM-2.1.4 **The licensee must not outsource the following functions:**

(i) Compliance;
(ii) AML/CFT;
(iii) Financial control;
(iv) Risk management; and
(v) Business line functions offering regulated services directly to the customers (refer to Regulation No. (1) of 2007 and its amendments for the list of CBB regulated services).

OM-2.1.5 **For the purposes of Paragraph OM-2.1.4, certain support activities, processes and systems under these functions may be outsourced (e.g. call centres, data processing, credit recoveries, cyber security, e-KYC solutions) subject to compliance with Paragraph OM-2.1.7. However, strategic decision-making and managing and bearing the principal risks related to these functions must remain with the licensee.**

OM-2.1 Outsourcing Arrangements (continued)

OM-2.1.6 Branches of foreign entities may be allowed to outsource to their head office, the risk management function stipulated in Subparagraph OM-2.1.4 (iv), subject to CBB's prior approval.

OM-2.1.7 **Licensees must comply with the following requirements:**

(i) Prior CBB approval is required on any outsourcing to a third-party outside Bahrain (excluding cloud data services). The request application must:

a. include information on the legal and technical due diligence, risk assessment and detailed compliance assessment; and

b. be made at least 30 calendar days before the licensee intends to commit to the arrangement.

(ii) Post notification to the CBB, within 5 working days from the date of signing the outsourcing agreement, is required on any outsourcing to an intragroup entity within or outside Bahrain or to a third-party within Bahrain, provided that the outsourced service does not require a license, or to a third-party cloud data services provider inside or outside Bahrain.

(iii) Licensees must have in place sufficient written requirements in their internal policies and procedures addressing all strategic, operational, logistical, business continuity and contingency planning, legal and risks issues in relation to outsourcing.

(iv) Licensees must sign a service level agreement (SLA) or equivalent with every outsourcing service provider. The SLA must clearly address the scope, rights, confidentiality and encryption requirements, reporting and allocation of responsibilities. The SLA must also stipulate that the CBB, external auditors, internal audit function, compliance function and where relevant the Shari'a coordination and implementation and internal Shari'a audit functions of the licensee have unrestricted access to all relevant information and documents maintained by the outsourcing service provider in relation to the outsourced activity.

(v) Licensees must designate an approved person to act as coordinator for monitoring and assessing the outsourced arrangement to ensure compliance with the licensee's internal policies and applicable laws and regulations.

(vi) Licensee must submit to the CBB any report by any other regulatory authority on the quality of controls of an outsourcing service provider immediately after its receipt or after coming to know about it.

OM-2.1 Outsourcing Arrangements (continued)

(vii) Licensee must inform its normal supervisory point of contact at the CBB of any material problems encountered with the outsourcing service provider if they remain unresolved for a period of three months from its identification date.

(viii) Where the internal audit function is fully or partially outsourced, licensees must ensure that:

i. The use of external experts does not compromise the independence and objectivity of the internal audit function;

ii. The outsourcing service provider has not been previously engaged in a consulting or external audit engagement with the licensee unless a one year "cooling-off" period has elapsed;

iii. The outsourcing service provider must not provide consulting services to the licensee during the engagement period; and

iv. Adequate oversight is maintained over the outsourcing service provider to ensure that it complies with the licensee's internal audit charter, policy and applicable laws and regulations.

OM-2.1.8 For the purpose of Subparagraph OM-2.1.7 (iv), licensees as part of their assessments may use the following:

a) Independent third-party certifications on the outsourcing service provider's security and other controls;
b) Third-party or internal audit reports of the outsourcing service provider; and
c) Pooled audits organized by the outsourcing service provider, jointly with its other clients.

When conducting on-site examinations, licensees should ensure that the data of the outsourcing service provider's other clients is not negatively impacted, including impact on service levels, availability of data and confidentiality.

OM-2.1.9 For the purpose of Subparagraph OM-2.1.7 (i), the CBB will provide a definitive response to any prior approval request for outsourcing within 10 working days of receiving the request complete with all the required information and documents.

OM-3.1 Board and Management Oversight

OM-3.1.1 This section sets out the requirements related to systems risk management and controls relevant to services offered through electronic banking activities and electronic funds transfer. Such services are prone to technical complexity, operational and security issues.

OM-3.1.2 **The Board of Directors, or a designated Board Committee and senior management must establish effective management oversight over the risks associated with activities involving e-banking and electronic funds transfer. The licensee must establish policies and procedures to manage these risks which include but are not be limited to the following:**

(a) The development and/or acquisition of the technology solutions;
(b) Testing of application program interfaces;
(c) Standards of communication and access and security of communication sessions, such as PCI-DSS compliance for cards;
(d) Authentication of the users;
(e) Processes and measures that protect customer data confidentiality consistent with Law No. 30 of 2018, Personal Data Protection Law (PDPL) issued on 12 July 2018;
(f) The use of enhanced fraud monitoring of movements in customers' accounts to guard against electronic frauds using various tools and measures, such as limits on value, volume and velocity; and
(g) Security policy and risk management controls.

OM-3.1.3 **The Board of Directors and senior management must ensure they possess the required competence, experience and skills to oversee, review and approve the key aspects of the licensee's security control process.**

OM-3.1.4 **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.**

OM-3.2 Secure Authentication

OM-3.2.1 **Licensees must take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business.**

OM-3.2.2 **Licensees must use predefined transaction authentication methods that promote non-repudiation and establish accountability for the transactions. Licensees must establish detailed procedures to effectively identify the person originating electronic funds transfer transactions and for 'call backs' when appropriate to avoid frauds in electronic fund transfers.**

OM-3.2.3 The term 'authentication' as used in this Module refers to the techniques, procedures and processes used to verify the identity and authorisation of prospective and established customers.

a) Identification refers to the procedures, techniques and processes used to establish the identity of a customer;
b) Authorisation refers to the procedures, techniques and processes used to determine that a customer or an employee has legitimate access to the bank account or the authority to conduct associated transactions on that account.

OM-3.2.4 **Licensees must have in place a strong customer authentication process for its e-banking activities which ensure the following:**

(a) no information on any of the elements of the strong customer authentication process can be derived from the disclosure of the authentication code;
(b) it is not possible to generate a new authentication code based on the knowledge of any other code previously generated; and
(c) the authentication code cannot be forged.

OM-3.2.5 The CBB will consider application of quantitative thresholds below which the strong customer authentication requirements may be simplified on a case-to-case basis.

OM-3.2.6 **Licensees must establish adequate security features for customer authentication including the use of the following three elements:**

(a) an element categorised as knowledge (something only the user knows), such as length or complexity of the pin or password;
(b) an element categorised as possession (something only the user possesses) such as algorithm specifications, key length and information entropy, and
(c) for the devices and software that read, elements categorised as inherence (something the user is), i.e. algorithm specifications, biometric sensor and template protection features.

OM-3.3 Other Systems and Controls

OM-3.3.1 Licensees must ensure that appropriate measures are in place to promote adequate segregation of duties within electronic funds transfer and e-banking systems, databases and applications.

OM-3.3.2 Licensees must ensure that proper authorisation controls and access privileges are in place for electronic funds transfer and e-banking systems, databases and applications.

OM-3.3.3 Licensees must ensure that appropriate measures are in place to protect the data integrity of all transactions, records and information.

OM-3.3.4 Licensees must ensure that clear audit trails exist for all electronic funds transfer and e-banking transactions.

OM-3.3.5 Licensees must establish and document the log retention requirements, including the identification of the source of each request, time synchronization of all related systems and all meta-data related to each request.

OM-3.3.6 Licensees must take appropriate measures to preserve the confidentiality of information. Measures taken to preserve confidentiality must be commensurate with the sensitivity of the information being transmitted and/or stored in databases.

OM-3.3.7 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-3.3.8 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-3.3.9 Licensees must have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.

OM-3.3.10 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-3.3 Other Systems and Controls (continued)

OM-3.3.11 Licensees must have in place customer awareness communications, pre and post onboarding process, using video calls, short videos or pop-up messages, to alert and warn natural persons applying to open current or saving accounts, credit, debit or prepaid cards or digital wallets about the risk of electronic frauds, and emphasise the need to secure their personal account details and not share them with anyone, online or offline.

OM-4.1 Introduction

OM-4.1.1 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.

OM-4.1.2 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 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.

Scope and Key Elements of a Business Continuity Management (BCM)

OM-4.1.3 **The requirements of this Chapter apply to all licensees.**

OM-4.1.4 Branches of foreign banks may apply alternative arrangements to those specified in this module, where they are subject to comprehensive BCM 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.

OM-4.2 General Requirements

OM-4.2.1 **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 establish a comprehensive framework for business continuity management (BCM) and 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-4.2.2 **Effective BCM framework must incorporate policy, procedures and tools required to manage the risk of major operational disruptions. The BCP 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-4.2.3 **Licensees must notify the CBB promptly if there are events that lead to activating their BCP. They must also provide regular progress reports, as agreed with the CBB, until the BCP is deactivated.**

OM-4.2.4 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-4.2.5 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-4.3 Board and Senior Management Responsibilities

Establishment of a Policy, Processes & Responsibilities

OM-4.3.1 A licensee's Board of Directors and Senior Management are collectively responsible for a bank's business continuity. The Board must approve the policies, while senior management must approve procedures and processes for a licensee's BCP.

OM-4.3.2 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-4.3.3 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-4.3.4 The CMT must submit regular reports to the Board and senior management on recovery and response activities in the event of major operational disruptions and also on the results of the testing of the BCP (refer to section OM-4.9). Major changes must be developed by CMT, reported to senior management, and endorsed by the Board.

OM-4.3.5 The Chief Executive of a licensee must sign a formal annual statement submitted to the Board on whether the response and recovery strategies adopted are still valid and whether the documented BCP is properly tested and maintained. The annual statement must be included in the BCM documentation and will be reviewed as part of the CBB's on-site examinations.

OM-4.4 Developing a Business Continuity Plan

Impact Analysis

OM-4.4.1 **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-4.4.2 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-4.4.3 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-4.4.4 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-4.4.5 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-4.4.6 **In developing a BCP, licensees must consider realistic threat scenarios that may (potentially) cause disruptions to their business processes.**

OM-4.4 Developing a Business Continuity Plan (continued)

OM-4.4.7 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-4.4.8 **BCPs must take into account different types of likely or plausible scenarios to which the bank may be vulnerable considering both the control (pre-event) measures and response (post-event) measures. In particular, the following specific scenarios must at a minimum, be considered in the BCP:**

(a) Utilities are not available (power, telecommunications);
(b) Critical buildings are not available or specific facilities are not accessible;
(c) Software and live data are not available or are corrupted;
(d) Vendor assistance or (outsourced) service providers are not available;
(e) Critical documents or records are not available;
(f) Critical personnel are not available; and
(g) Significant equipment malfunctions (hardware or telecom).

OM-4.4.9 **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-4.4.10 **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-4.5 Recovery Levels & Objectives

OM-4.5.1 **The BCM framework must include strategies and procedures to maintain, resume and recover critical business operations or services. The plan must differentiate between critical and non-critical functions. The BCM policy 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-4.5.2 **The BCM policy 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-4.5.3 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-4.5.4 **Individual critical business and support functions must establish Recovery Time Objectives (RTO), Recovery Point Objectives (RPO) and Maximum Tolerable Period of Disruption (MTPD) with respect to the bank's recovery programme. RTOs, RPOs and MTPDs must be approved by the senior management prior to proceeding to the development of the BCP.**

List of Contacts and Responsibilities

OM-4.5.5 **The BCM framework must consider a communication strategy, established procedures for communication, methodology for transmitting, writing and reading of relevant information designed for each business unit where appropriate, the nature of information a list of all key resources charged with the tasks and the full listing of employees and relevant stakeholders. 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-4.5 Recovery Levels & Objectives (continued)

OM-4.5.6 **The BCM policy 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-4.5.7 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-4.5.8 **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-4.5.9 **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-4.5.10 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-4.5 Recovery Levels & Objectives (continued)

OM-4.5.11 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-4.5.12 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-4.5.13 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-4.5.14 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-4.6 Detailed Procedures for the BCP

OM-4.6.1 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-4.6.2 **A BCM framework must include 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-4.6 Detailed Procedures for the BCP (continued)

OM-4.6.3 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-4.6.4 **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-4.6.5 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 business resumption process.

OM-4.6.6 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 BCM framework.

Technology Recovery

OM-4.6.7 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-4.6 Detailed Procedures for the BCP (continued)

OM-4.6.8 Licensees should pay attention to Heat, Ventilation and Air Conditioning (HVAC) requirements and 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-4.6.9 **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-4.6.10 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-4.6.11 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-4.6.12 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-4.6.13 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-4.7 Vital Records Management

OM-4.7.1 Each BCM framework 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-6 when identifying vital information for business continuity. Vital information includes information stored on both electronic and non-electronic media.

OM-4.7.2 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-4.8 Other Policies Standards, and Processes

Employee Awareness and Training Plan

OM-4.8.1 **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-4.8.2 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-4.8.3 **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-4.8.4 **The BCM framework 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-4.8.5 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-4.8 Other Policies, Standards and Processes (continued)

OM-4.8.6 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-4.8.7 **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-4.8.8 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-4.8.9 **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. In all cases, BCP disclosures must be reviewed and updated to address changes to the BCP.**

OM-4.8.10 The licensees might make these disclosures on their websites, or through mailing to key external parties upon request.

OM-4.9 Maintenance, Testing and Review

Testing & Rehearsal

OM-4.9.1 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-4.9.2 **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-4.9.3 **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 backup 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-4.9 Maintenance, Testing and Review (continued)

OM-4.9.4 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-4.9.5 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, an assessment 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 annual assessment of the appropriateness of the relevant service level agreements.

OM-4.9.6 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-4.9.7 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-4.9 Maintenance, Testing and Review (continued)

OM-4.9.8 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-4.9.9 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-4.9.10 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.

OM-4.9.11 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-5.1 Security Measures for Retail Banks

General Requirement

OM-5.1.1 **Retail banks must maintain up to date Payment Card Industry Data Security Standards (PCI-DSS) certification. 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-5.1.2 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.

OM-5.1.2A **Islamic retail bank licensees must take appropriate measures to counter fraudulent phishing attempts (such as through telephone or WhatsApp calls, SMS or WhatsApp messages, emails and other media) that request customers to provide sensitive personal information that can lead to frauds. The licensees must also enhance their surveillance and monitoring systems to detect suspicious account activity caused by such fraudulent attempts on a timely basis.**

OM-5.1.2B **Islamic retail bank licensees must raise customer awareness about fraudulent phishing messages by launching extensive customer alert campaigns through media and social media channels. Customers must be warned of such attempts and advised to only use the licensee's official website, telephone or other channels for communication with it.**

External Measures

OM-5.1.3 **All head offices/main offices are required to maintain Ministry of Interior ("MOI") guards on a 24 hours basis. For branches that satisfy the criteria mentioned in Paragraphs OM-5.1.4 to OM-5.1.16 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.**

OM-5.1 Security Measures for Retail Banks (continued)

OM-5.1.4 Public entrances to head offices/main offices and branches must be protected by 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) Multifactor or combination access control system (e.g. access card and key slot or swipe card and password).

OM-5.1.5 External windows must have security measures such as anti-blast films and movement detectors. For ground floor windows, banks must add steel grills fastened into the wall.

OM-5.1.6 Branch alarm systems must 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-5.1.7 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-5.1.8 All areas where cash is handled must be screened off from customers and other staff areas.

OM-5.1.9 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-5.1.10 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-5.1 Security Measures for Retail Banks (continued)

Cash Safety

OM-5.1.11 Cash, precious metals and bearer instruments must be kept in fireproof cabinets/safes. These cabinets/safes must be located in strong rooms.

OM-5.1.12 Strong rooms must be made of reinforced solid concrete, or reinforced block work. Doors to strong rooms must be steel and 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-5.1.13 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.

CCTV Network Systems

OM-5.1.14 All head offices/main offices and branches must have a CCTV network and alarm system which are connected to a central monitoring unit located in the head office/main office, along with a Video Monitoring System (VMS) and to the MOI Central Monitoring Unit.

OM-5.1.15 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-5.3 for specific CCTV requirements related to ATMs.

OM-5.1.16 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-5.1 Security Measures for Retail Banks (continued)

Training and Other Measures

OM-5.1.17 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-5.1.18 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-5.1.19 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-5.2 Payment and ATM cards, Wallets and Point of Sale infrastructure

Europay, MasterCard and Visa (EMV) Compliance

OM-5.2.1 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 BD50 per transaction, provided that Islamic bank licensees bear full responsibility in case of fraud occurrence.

OM-5.2.1A Where contactless payments use Consumer Device Cardholder Verification Method (CDCVM) for payment authentication and approval, then the authentication required for transactions above BD50 limit mentioned in Paragraph OM-5.2.1 is not applicable given that the customer has already been authenticated by his device using PIN, biometric or other authentication methods. This is only applicable where debit/credit card of the customer has already been tokenized in the payment application.

Provision of Cash Withdrawal and Payment Services through Various Channels

OM-5.2.2 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 explicit consent from the customers using established methods described in OM-3.2 and enrolling them through a registration process for each channel and service, wherein customers' acceptance of products/services terms and conditions are documented and customers are properly authenticated. Such enrolment process must allow an opt-out option if the customer does not want to use a channel for which he has enrolled.

OM-5.2 Payment and ATM cards, Wallets and Point of Sale infrastructure (Continued)

Geolocation Limitations

OM-5.2.3 **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).**

Prohibition of Double Swiping

OM-5.2.4 **Double swiping of cards by merchants is not allowed, and all card acquirer licensees must ensure that the merchants concerned must comply with this requirement.**

OM-5.2.5 For the purpose of Paragraph OM-5.2.4, 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-5.2.6 For the purpose of Paragraph OM-5.2.4, 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-5.2.7 **All card acquirer licensees must include the following clause into the merchant agreements entered into with all their merchants: "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-5.2 Payment and ATM cards, Wallets and Point of Sale infrastructure (Continued)

OM-5.2.8 All card acquirer licensees must:

(i) Educate the concerned merchants on the regulatory requirement and monitor the implementation of this requirement; 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-5.2.9 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-5.2.10 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-5.2.11 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-5.2.12 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-5.2 Payment and ATM cards, Wallets and Point of Sale infrastructure (Continued)

OM-5.2.13 Banks must ensure that the integration of Secure Card Readers, (SCRs) and, if applicable, any mechanism protecting the SCRs and any anti skimming devices are properly implemented and fully comply with the guidelines provided by the device vendor. SCRs must be PCI Security Standards Council approved and fully comply with all PCI standards at all times.

OM-5.2.14 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-5.2.15 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;

(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;

(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

OM-5.2 Payment and ATM cards, Wallets and Point of Sale infrastructure (continued)

(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-5.2.16 ATMs must incorporate dedicated tampering protection capabilities.

ATM Application Management

OM-5.2.17 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.

MODULE	OM:	Operational Risk Management
CHAPTER	OM-5:	Security Measures for Banks

OM-5.3 ATM Security Measures: Physical Security for Retail Banks

Record Keeping

OM-5.3.1 **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-5.3.2 **Banks must notify the CBB in writing if they install a new off-site ATM or remove/terminate any of its off-site ATMs.**

OM-5.3.3 [This Paragraph was deleted in January 2022].

General Criteria

OM-5.3.4 **[This Paragraph was deleted in January 2022].**

OM-5.3.5 **[This Paragraph was deleted in January 2022].**

OM-5.3.6 **[This Paragraph was deleted in January 2022].**

OM-5.3.7 **[This Paragraph was deleted in January 2022].**

OM-5.3.8 [This Paragraph was deleted in January 2022].

OM-5.3.9 [This Paragraph was deleted in January 2022].

OM-5.3.10 [This Paragraph was deleted in January 2022].

OM-5.3.11 **[This Paragraph was deleted in January 2022].**

OM-5.3.12 The CBB may, at its sole discretion, require an off-site ATM to be removed/terminated and decommissioned at any time.

OM-5.3 ATM Security Measures: Physical Security for Retail Banks (continued)

ATM Alarms

OM-5.3.13 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 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-5.3 ATM Security Measures: Physical Security for Retail Banks (continued)

Closed-circuit Television (CCTV)

OM-5.3.14 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 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. There must be sensors to detect and alert the bank if the camera has been blocked or tampered with.

OM-5.3.15 For the purposes of Paragraph OM-5.3.14, 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-5.3.16 As a minimum, CCTV activity must be recorded (preferably in digital format) and, where risk dictates, remotely monitored by a third-party Alarm Receiving Centre.

OM-5.3.17 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-5.3.18 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-5.3 ATM Security Measures: Physical Security for Retail Banks (continued)

OM-5.3.19 **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-5.3.20 **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-5.3.21 **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 during both daytime and nighttime.**

Fire Alarm

OM-5.3.22 **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.**

Cash Replenishment

OM-5.3.23 **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-5.3.24 **Banks must maintain a list of all maintenance, replenishment and inspection visits by staff or other authorised parties.**

OM-5.3.25 The CBB shall conduct inspections of ATM installations and any non-compliance with the physical security requirements stipulated in this Chapter may lead to suspension of the subject ATMs and trigger other enforcement measures set out in Module EN.

OM-5.4 ATM Security Measures: Additional Measures for Retail Banks

OM-5.4.1 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-5.4.2 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-5.4.3 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-5.5 Cyber Security Risk Management

Role of the Board

OM-5.5.1 **The Board of Islamic bank licensees must ensure that the licensee has a robust cyber security risk management policy to comprehensively manage the licensee's cyber security risk and vulnerabilities. The Board must approve the policy and establish clear ownership, decision-making and management accountability for risks associated with cyber-attacks and related risk management and recovery processes. Cyber security must be an item for discussion at Board or Board sub-committee meetings.**

OM-5.5.2 **The Board of Islamic bank licensees must ensure that the cyber security risk management framework encompasses, at a minimum, the following components:**

a) Cyber security strategy;
b) Cyber security policy; and
c) Cyber security risk management approach, tools and methodology and, an organization-wide security awareness program.

OM-5.5.3 **The cyber security risk management framework must be developed in accordance with the National Institute of Standards and Technology (NIST) Cyber security framework which is summarized in Appendix C – Cyber security Control Guidelines. At the broader level, the Cyber security framework should be consistent with the licensee's risk management framework.**

OM-5.5.4 Boards should receive comprehensive reports, in every Board meeting, covering cyber security issues such as the following:

a. Key Risk Indicators/ Key Performance Indicators;
b. Status reports on overall cyber security control maturity levels;
c. Status of staff Information Security awareness;
d. Updates on latest internal or relevant external cyber security incidents; and
e. Results from penetration testing exercises.

OM-5.5.5 **The Board must evaluate and approve the cyber security risk management framework for scope coverage, adequacy and effectiveness every three years or when there are significant changes to the risk environment, taking into account emerging cyber threats and cyber security controls.**

OM-5.5 Cyber Security Risk Management (continued)

OM-5.5.6 **Islamic bank licensees must establish a cyber security risk function, independent of the information technology (IT) department, which must report to an independent risk management function or an equivalent function within the licensee. The cyber security risk management function must monitor and report on the status and maturity of relevant cyber security controls. Branches of foreign bank licensees must be governed under a framework of cyber security risk management policies which ensure that an adequate level of oversight is exercised by the regional office or head office.**

OM-5.5.7 The Board should ensure that appropriate resources are allocated to the cyber security risk management function for implementing the cyber security framework.

OM-5.5.8 **The Board must ensure that the cyber security risk management function is headed by suitably qualified Chief Information Security Officer (CISO), with appropriate authority to implement the Cyber Security strategy.**

OM-5.5.9 The Board should establish a cyber security committee that is headed by an independent senior manager from a control function (like CFO / CRO), with appropriate authority to approve policies and frameworks needed to implement the cyber security strategy, and act as a governance committee for the cyber security function. Membership of this committee should include senior management members from business functions, IT, Risk and Compliance.

OM-5.5 Cyber Security Risk Management (continued)

Role of Senior Management

OM-5.5.10 The senior management must be responsible for the following activities:

(a) Create the overall cyber security risk management framework and adequately oversee its implementation;
(b) Formulate a bank-wide cyber security strategy and cyber security policy;
(c) Implement and consistently maintain an integrated, bank-wide, cyber security risk management framework, and ensure sufficient resource allocation;
(d) Monitor the effectiveness of the implementation of cyber security risk management practices and coordinate cyber security activities with internal and external risk management entities;
(e) Provide quarterly or more frequent reports to the Board on the current situation with respect to cyber threats and cyber security risk treatment;
(f) Prepare quarterly or more frequent reports on all cyber incidents (internal and external) and their implications on the licensee; and
(g) Ensure that processes for identifying the cyber security risk levels across the organisation are in place and annually evaluated.

OM-5.5.11 The senior management must ensure that:

(a) The licensee has identified clear internal ownership and classification for all information assets and data;
(b) The licensee has maintained an inventory of the information assets and data which is reviewed and updated regularly;
(c) The cyber security staff are adequate to manage the licensee's cyber security risks and facilitate the performance and continuous improvement of all relevant cyber security controls;
(d) It provides and requires cyber security staff to attend regular cyber security update and training sessions (for example Security+, CEH, CISSP, CISA, CISM) to stay abreast of changing cyber security threats and countermeasures.

OM-5.5 Cyber Security Risk Management (continued)

OM-5.5.12 With respect to Subparagraph OM-5.5.11(a), data classification entails analyzing the data the licensee retains, determining its importance and value, and then assigning it to a category. When classifying data, the following aspects of the policy should be determined:

a) Who has access to the data;
b) How the data is secured;
c) How long the data is retained (this includes backups);
d) What method should be used to dispose of the data;
e) Whether the data needs to be encrypted; and
f) What use of the data is appropriate.

The general guideline for data classification is that the definition of the classification should be clear enough so that it is easy to determine how to classify the data. In other words, there should be little (if any) overlap in the classification definitions. The owner of data (i.e. the relevant business function) should be involved in such classification.

Cyber Security Strategy

OM-5.5.13 **A bank-wide cyber security strategy must be defined and documented to include:**

a) The position and importance of cyber security at the licensee;
b) The primary cyber security threats and challenges facing the licensee;
c) The licensee's approach to cyber security risk management;
d) The key elements of the cyber security strategy including objectives, principles of operation and implementation approach;
e) Scope of risk identification and assessment, which must include the dependencies on third party service providers;
f) Approach to planning response and recovery activities; and
g) Approach to communication with internal and external stakeholders including sharing of information on identified threats and other intelligence among industry participants.

OM-5.5.14 The cyber security strategy should be communicated to the relevant stakeholders and it should be revised as necessary and, at least, once every three years. Appendix C provides cyber security control guidelines that can be used as reference to support the licensee's cyber security strategy and cyber security policy.

OM-5.5 Cyber Security Risk Management (continued)

Cyber Security Policy

OM-5.5.15 Islamic bank licensees must implement a written cyber security policy setting forth its policies for the protection of its electronic systems and client data stored on those systems, which must be reviewed and approved by the licensee's board of directors or senior management, as appropriate, at least annually. The cyber security policy areas including but not limited to the following must be addressed:

(a) Definition of the key cyber security activities within the licensee, the roles, responsibilities, delegated powers and accountability for these activities;

(b) A statement of the licensee's overall cyber risk tolerance as aligned with the licensee's business strategy. The cyber risk tolerance statement should be developed through consideration of the various impacts of cyber threats including customer impact, service downtime, potential negative media publicity, potential regulatory penalties, financial loss, and others;

(c) Definition of main cyber security processes and measures and the approach to control and assessment;

(d) Policies and procedures (including process flow diagrams) for all relevant cyber security functions and controls including the following:

(a) Asset management (Hardware and software);
(b) Incident management (Detection and response);
(c) Vulnerability management;
(d) Configuration management;
(e) Access management;
(f) Third party management;
(g) Secure application development;
(h) Secure change management;
(i) Cyber training and awareness;
(j) Cyber resilience (business continuity and disaster planning); and
(k) Secure network architecture.

OM-5.5 Cyber Security Risk Management (continued)

Approach, Tools and Methodology

OM-5.5.16 **Islamic bank licensees must ensure that the cyber security policy is effectively implemented through a consistent risk-based approach using tools and methodologies that are commensurate with the size and risk profile of the licensee. The approach, tools and methodologies must cover all cyber security functions and controls defined in the cyber security policy.**

OM-5.5.17 Licensees should establish and maintain plans, policies, procedures, process and tools ("playbooks") that provide well-defined, organised approaches for cyber incident response and recovery activities, including criteria for activating the measures set out in the plans and playbooks to expedite the organisation's response time. Plans and playbooks should be developed in consultation with business lines to ensure business recovery objectives are met and are approved by senior management before broadly shared across the licensee. They should be reviewed and updated regularly to incorporate improvements and/or changes in the organisation. Licensees may enlist external subject matter experts to review complex and technical content in the playbook, where appropriate. A number of plans and playbooks should be developed for specific purposes (e.g. response, recovery, contingency, communication) that align with the overall cyber security strategy.

Prevention Controls

OM-5.5.18 **A Islamic bank licensee must develop and implement preventive measures across all relevant technologies to minimise the licensee's exposure to cyber security risk. Such preventive measures must include, at a minimum, the following:**

(a) Deployment of End Point Protection (EPP) and Endpoint Detection and Response including anti-virus software and anti-malware programs to detect, prevent, and isolate malicious code;

(b) Data leakage prevention solutions to detect and prevent confidential data from leaving the licensee's technology environment;

(c) Use of firewalls for network segmentation including use of Web Application Firewalls (WAF) for filtering and monitoring HTTP traffic between a web application and the Internet, and access control lists to limit unauthorized system access between network segments;

(d) Rigorous security testing at software development stage as well as after deployment to limit the number of vulnerabilities;

(e) Use of Privileged Access Management (PAM) to secure, control, manage and monitor privileged access to critical assets;

OM-5.5 Cyber Security Risk Management (Continued)

(f) Use of a secure email gateway to limit email based cyber-attacks such as malware attachments, malicious links, and phishing scams (for example use of Microsoft Office 365 Advanced Threat Protection tools for emails);
(g) Use of a Secure Web Gateway to limit browser based cyber-attacks, malicious websites and enforce organization policies;
(h) Creating a list of whitelisted applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on the organization's systems;
(i) Use of mobile device management solutions including implementing Bring Your Own Device "BYOD" security policies to secure all mobile devices with any access to bank systems, applications, and networks through security measures such as encryption, remote wipe capabilities, and password enforcement; and
(j) Network access control to secure physical network ports against connection to computers which are unauthorised to connect to the licensee's network or which do not meet the minimum-security requirements defined for licensee computer systems; and
(k) Identity and access management solutions to limit the exploitation and monitor the use of privileged and non-privileged accounts.

OM-5.5.19 Islamic bank licensees must set up anti-spam and anti-spoofing measures to authenticate the licensee's mail server and to prove to ISPs, mail services and other receiving mail servers that senders are truly authorized to send the email. Examples of such measures include:

- SPF "Sender Policy Framework";
- DKIM "Domain Keys Identified Mail"; and
- DMARC "Domain-based Message Authentication, Reporting and Conformance".

OM-5.5.20 Islamic bank licensees should subscribe to one of the Cyber Threat Intelligence services in order to stay abreast of emerging cyber threats, cybercrime actors and state of the art tools and security measures.

OM-5.5 Cyber Security Risk Management (Continued)

OM-5.5.21 **Islamic bank licensees must use a single unified private email domain or its subdomains for communication with customers to prevent abuse by third parties. Licensees must not utilise third-party email provider domains for communication with customers. The email domains must comply with the requirements with respect to SPF, DKIM and DMARC in this Module. With respect to URLs or other clickable links in communications with customers, licensees must comply with the following requirements:**

(a) Limit the use of links in SMS and other short messages (such as WhatsApp) to messages sent as a result of customer request or action. Examples of such customer actions include verification links for customer onboarding, payment links for customer-initiated transactions etc;

(b) Refrain from using shortened links in communication with customers;

(c) Implement one or more of the following measures for links sent to customers:

i. ensure customers receive clear instructions in communications sent with the links;

ii. prior notification to the customer such as through a phone call informing the customer to expect a link from the licensee;

iii. provision of transaction details such as the transaction amount and merchant name in the message sent to the customer with the link;

iv. use of other verification measures like password or biometric authentication; and

(d) Create customer awareness campaigns to educate their customers on the risk of fraud related to links they receive in SMS, short messages and emails with clear instructions to customers that licensees will not send clickable links in SMS, emails and other short messages to request information or payments unless it is as a result of customer request or action.

OM-5.5.21A For the purpose of Paragraph OM-5.5.21, subject to CBB's approval, licensees may be allowed to use additional domains for email communications with customers under certain circumstances. Examples of such circumstances include emails sent to customers by:

(a) Head/regional office of a licensee; and

(b) Third-party service providers subject to prior arrangements being made with customers. Examples of such third-party services include informational subscription services (e.g. Bloomberg) and document management services (e.g. DocuSign).

OM-5.5 Cyber Security Risk Management (continued)

Cyber Risk Identification and Assessments

OM-5.5.22 **Islamic bank licensees must conduct periodic assessments of cyber threats. For the purpose of analysing and assessing current cyber threats relevant to the licensee, it should take into account the factors detailed below:**

(a) Cyber threat entities including cyber criminals, cyber activists, insider threats;

(b) Methodologies and attack vectors across various technologies including cloud, email, websites, third parties, physical access, or others as relevant;

(c) Changes in the frequency, variety, and severity of cyber threats relevant to the region;

(d) Dark web surveillance to identify any plot for cyber-attacks;

(e) Examples of cyber threats from past cyber-attacks on the licensee if available; and

(f) Examples of cyber threats from recent cyber-attacks on other organisations.

OM-5.5.23 **Islamic bank licensees must conduct periodic assessments of the maturity, coverage, and effectiveness of all cyber security controls. Cyber security control assessment must include an analysis of the controls' effectiveness in reducing the likelihood and probability of a successful attack.**

OM-5.5.24 Licensees should ensure that the periodic assessments of cyber threats and cyber security controls cover all critical technology systems. A risk treatment plan should be developed for all residual risks which are considered to be above the licensee's risk tolerance levels.

OM-5.5.25 **Islamic bank licensees must conduct regular technical assessments to identify potential security vulnerabilities for systems, applications, and network devices. The vulnerability assessments must be comprehensive and cover internal technology, external technology, and connections with third parties. Preferably monthly assessments are conducted for internal technology and weekly or more frequent assessments for external public facing services and systems.**

OM-5.5 Cyber Security Risk Management (continued)

OM-5.5.26 With respect to Paragraph OM-5.5.25, external technology refers to the licensee's public facing technology such as websites, apps and external servers. Connections with third parties includes any API or other connections with fintech companies, technology providers, outsourcing service providers etc.

OM-5.5.27 **Islamic bank licensees must have in place vulnerability and patch management processes which include remediation processes to ensure that the vulnerabilities identified are addressed and that security patches are applied where relevant within a timeframe that is commensurate with the risks posed by each vulnerability.**

OM-5.5.28 **All licensees must perform penetration testing of their systems, applications, and network devices to verify the robustness of the security controls in place at least twice a year. These tests must be used to simulate real world cyber-attacks on the technology environment and must:**

(a) Follow a risk-based approach based on an internationally recognized methodology, such as National Institute of Standards and Technology "NIST" and Open Web Application Security Project "OWASP";

(b) Include both Grey Box and Black Box testing in its scope;

(c) Be conducted by qualified and experienced security professionals who are certified in providing penetration testing services;

(d) Be performed by internal and external independent third parties which should be changed at least every two years; and

(e) Be performed on either the production environment or on non-production exact replicas of the production environment.

OM-5.5.29 CBB may require additional red teaming exercises to be performed as needed. A red team is a group of ethical hackers with varying backgrounds, that would test the organization's blue team's threat response activity. The red team may attack 3 fronts: cyber, social (attack on people's behavior) and physical (attack on an organization's physical facility and or 3rd party premises). A red teaming exercise is like a penetration test in many ways but more targeted. The goal is not to find as many vulnerabilities as possible. The goal is to test the organization's detection and response capabilities. The red team will try to get in and access sensitive information in any way possible, as quietly as possible.

OM-5.5.30 **Where licensees have been required to conduct a red teaming exercise the results of such an exercise must be provided to CBB within one month of the completion of the exercise together with a comprehensive plan to address any observed weaknesses.**

OM-5.5 Cyber Security Risk Management (continued)

Cyber Incident Detection and Management

OM-5.5.31 **Islamic bank licensees must implement cyber security incident management processes to ensure timely detection, response and recovery for cyber security incidents. This includes implementing a Security Information & Event Management "SIEM" system.**

OM-5.5.32 Licensees should consider the adequacy of the SIEM, keeping in view it should receive data on a real time basis from all relevant systems, applications, and network devices including operational and business systems. The monitoring system should be capable of identifying indicators of cyber incidents and initiate alerts, reports, and response activities based on the defined cyber security incident management process.

OM-5.5.33 Licensees should retain the logs and other information from the SIEM for detecting cyber incidents, including "low-and-slow" attacks, in order to facilitate incident investigations, for 5 years or longer.

OM-5.5.34 Once a cyber incident is detected, licensees should activate their containment measures, processes and technologies best suited to each type of cyber incident to prevent a cyber incident from inflicting further damage. This may involve, after considering the costs, business impact and operational risks, shutting down or isolating all or affected parts of their systems and networks as deemed necessary for containment and diagnosis.

OM-5.5.35 **Islamic bank licensees must establish a Security Operations Centre (SOC) that is tailored to the needs of the licensee to detect, identify, investigate and respond to cyber incidents that could impact the licensee's infrastructure, services and customers. Capabilities for log collection and monitoring SIEM must be built into the SOC. The SOC must maintain the licensee's asset inventory and network diagrams.**

OM-5.5.36 **Islamic bank licensees must regularly identify, test, review and update current cyber security risk scenarios and the corresponding response plan. This is to ensure that the scenarios and response plan remain relevant and effective, taking into account changes in the operating environment, systems or the emergence of new cyber security threats. If any gaps are identified, the SIEM system must be updated with new use cases and rule sets which are capable of detecting the current cyber incident scenarios.**

OM-5.5 Cyber Security Risk Management (continued)

OM-5.5.37 The cyber incident scenario tests should include high-impact-low-probability events and scenarios that may result in failure. Common cyber incident scenarios include distributed denial of service (DDoS) attacks, system intrusion, data exfiltration and system disruption. Licensees should regularly use threat intelligence to update the scenarios so that they remain current and relevant. Licensees should periodically review current cyber incident scenarios for the purpose of assessing the licensee's ability to detect and respond to these scenarios if they were to occur.

OM-5.5.38 **Islamic bank licensees must ensure that critical cyber security incidents detected are escalated to an incident response team, management and the Board, in accordance with the licensee's business continuity plan and crisis management plan, and that an appropriate response is implemented promptly. See also Paragraph OM-5.5.57 for the requirement to report to CBB.**

OM-5.5.39 Islamic bank licensees should clearly define the roles, responsibilities and accountabilities for cyber incident detection and response activities to one or more named individuals that meet the pre-requisite role requirements. Potential conflicts of interest are minimised by ensuring a separation of implementation and oversight roles where possible. The roles should include:

- **Incident Owner:** An individual that is responsible for handling the overall cyber incident detection and response activities according to the incident type and services affected. The Incident Owner is delegated appropriate authority to manage the mitigation or preferably, removal of all impacts due to the incident.
- **Spokesperson:** An individual, from External Communications Unit or another suitable department, that is responsible for managing the communications strategy by consolidating relevant information and views from subject matter experts and the organisation's management to update the internal and external stakeholders with consistent information.
- **Record Keeper:** An individual that is responsible for maintaining an accurate record of the cyber incident throughout its different phases, as well as documenting actions and decisions taken during and after a cyber incident. The record serves as an accurate source of reference for after-action reviews to improve future cyber incident detection and response activities.

OM-5.5.40 For the purpose of managing a critical cyber incident, the licensee should operate a situation room, and should include in the incident management procedure a definition of the authorities and responsibilities of staff members, internal and external reporting lines, communication channels, tools and detailed working procedures. The situation room or a war room is a physical room or a virtual room where relevant members of the management gather to handle a crisis in the most efficient manner possible.

OM-5.5 Cyber Security Risk Management (Continued)

OM-5.5.41 Licensees 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 licensee should maintain an "incident 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. It should also include the status of the issue whether it is open or has been resolved and person in charge of resolving the issue/incident. The logs should be stored and preserved in a secure and legally admissible manner.

OM-5.5.42 Licensees should utilise pre-defined taxonomy for classifying cyber incidents according to, for example, the type of incident, threat actors, threat vectors and repercussions; and a pre-established severity assessment framework to help gauge the severity of the cyber incident. For example, taxonomies that can be used when describing cyber incidents:

(a) Describe the cause of the cyber incident (e.g. process failure, system failure, human error, external event, malicious action);
(b) Describe whether the cyber incident due to a third-party service provider;
(c) Describe the attack vector (e.g. malware, virus, worm, malicious hyperlink);
(d) Describe the delivery channel used (e.g. e-mail, web browser, removable storage media);
(e) Describe the impact (e.g. service degradation/disruption, service downtime, potential impact to customers, data leakage, unavailability of data, data destruction/corruption, tarnishing of reputation);
(f) Describe the type of incident (e.g. zero-day attack, exploiting a known vulnerability, isolated incident);
(g) Describe the intent (e.g. malicious, theft, monetary gain, fraud, political, espionage, opportunistic);
(h) Describe the threat actor (e.g. script kiddies, amateur, criminal syndicate, hacktivist, nation state).

The cyber incident severity may be classified as:

(a) **Severity 1** incident has or will cause a serious disruption or degradation of critical service(s) and there is potentially high impact on public confidence in the licensee.
(b) **Severity 2** incident has or will cause some degradation of critical services and there is medium impact on public confidence in the licensee.
(c) **Severity 3** incident has little or no impact to critical services and there is no visible impact on public confidence in the licensee.

OM-5.5.43 Licensees should determine the effects of the cyber incident on customers and to the wider banking system as a whole and report the results of such an assessment to CBB if it is determined that the cyber incident may have a systemic impact. Licensees may also share non-sensitive information on cyber incidents, effective cyber security strategies and risk management practices through malware information sharing platforms (MISP). Technical information, such as Indicators of Compromise (IoCs) or vulnerabilities exploited can be shared through MISP.

OM-5.5 Cyber Security Risk Management (continued)

OM-5.5.44 Licensees should establish metrics to measure the impact of a cyber incident and to report to management the performance of response activities. Examples include:

1. Metrics to measure impact of a cyber incident:
   (a) Duration of unavailability of critical functions and services;
   (b) Number of stolen records or affected accounts;
   (c) Volume of customers impacted;
   (d) Amount of lost revenue due to business downtime, including both existing and future business opportunities;
   (e) Percentage of service level agreements breached.
2. Performance metrics for incident management:
   (a) Volume of incidents detected and responded via automation;
   (b) Dwell time (i.e. the duration a threat actor has undetected access until completely removed);
   (c) Recovery Point objectives (RPO) and recovery time objectives (RTO) satisfied.

Recovery

OM-5.5.45 **Islamic bank licensees must identify the critical systems and services within its operating environment that must be recovered on a priority basis in order to provide certain minimum level of services during the downtime and determine how much time the licensee will require to return to full service and operations.**

OM-5.5.46 Critical incidents are defined as incidents that trigger the BCP and the crisis management plan. Critical systems and services are those whose failure can have material impact on any of the following elements:

a) Financial situation;
b) Reputation;
c) Regulatory, legal and contractual obligations; and
d) Operational aspects and delivery of key products and services.

OM-5.5.47 **Islamic bank licensees must define a program for recovery activities for timely restoration of any capabilities or services that were impaired due to a cyber security incident. Licensees must establish recovery time objectives ("RTOs"), i.e. the time in which the intended process is to be covered, and recovery point objectives ("RPOs"), i.e. point to which information used must be restored to enable the activity to operate on resumption". Licensees must also consider the need for communication with third party service providers, customers and other relevant external stakeholders as may be necessary.**

OM-5.5 Cyber Security Risk Management (continued)

OM-5.5.48 **Islamic bank licensees must ensure that all critical systems are able to recover from a cyber security breach within the licensee's defined RTO in order to provide important services or some level of minimum services for a temporary period of time.**

OM-5.5.49 Licensees should validate that recovered assets are free of compromise, fully functional and meet the security requirements before returning the systems to normal business operations. This includes performing checks on data to ensure data integrity. In some cases, licensees may need to use backup data kept in a disaster recovery site or plan for the reconstruction of data from external stakeholders such as business partners and customers.

OM-5.5.50 **Islamic bank licensees must define a program for exercising the various response mechanisms, 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-5.5.51 **Islamic bank licensees must define the mechanisms for ensuring accurate, timely and actionable communication of cyber incident response and recovery activities with the internal stakeholders, including to the board or designated committee of the board.**

OM-5.5.52 **A Islamic bank licensee must ensure its business continuity plan is comprehensive and includes a recovery plan for its systems, operations and services arising from a cyber security incident.**

OM-5.5 Cyber Security Risk Management (continued)

Cyber Security Insurance

OM-5.5.53 Islamic bank licensees must arrange to seek cyber risk insurance cover from a suitable insurer, following a risk-based assessment of cyber security risk is undertaken by the respective licensee and independently verified by the insurance company. 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.

Training and Awareness

OM-5.5.54 Islamic bank licensees must evaluate improvement in the level of awareness and preparedness to deal with cyber security risk to ensure the effectiveness of the training programmes implemented.

OM-5.5.55 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'.

OM-5.5.56 The Islamic bank licensees must ensure that role specific cyber security training is provided on a regular basis to relevant staff including:

(a) Executive board and senior management;

(b) Cyber security roles;

(c) IT staff; and

(d) Any high-risk staff as determined by the licensee.

OM-5.5 Cyber Security Risk Management (continued)

Reporting to CBB

OM-5.5.57 **Upon occurrence or detection of any cyber security incident, whether internal or external, that compromises customer information or disrupts critical services that affect operations, Islamic bank licensees must contact the CBB, immediately (within one hour), on 17547477 and submit Section A of the Cyber Security Incident Report (Appendix OM-1) to CBB's cyber incident reporting email, incident.islamic@cbb.gov.bh, within two hours.**

OM-5.5.58 **Following the submission referred to in Paragraph OM-5.5.57, the licensee must submit to CBB Section B of the Cyber Security Incident Report (Appendix OM-1) within 10 calendar days of the occurrence of the cyber security incident. Licensees must include all relevant details in the report, including the full root cause analysis of the cyber security incident, its impact on the business operations and customers, and all measures taken by the licensee to stop the attack, mitigate its impact and to ensure that similar events do not recur. In addition, a weekly progress update must be submitted to CBB until the incident is fully resolved.**

OM-5.5.59 With regards to the submission requirement mentioned in Paragraph OM-5.5.58, the licensee should submit the report with as much information as possible even if all the details have not been obtained yet.

OM-5.5 Cyber Security Risk Management (continued)

OM-5.5.60 The comprehensive cyber security incident report referred to in Paragraph OM-5.5.58 should include the following details:

(a) Date and time of discovery of the incident;
(b) Time elapsed from detection to restoration of critical services;
(c) Who discovered the incident (e.g. third-party service provider, customer, employee);
(d) Type of cyber incident (e.g. DDoS, malware, intrusion/unauthorised access, hardware/firmware failure, system software bugs;)
(e) Impact of the incident (e.g. impact to availability of services, loss of confidential information) including financial, legal and reputational impact and to which group of stakeholders (e.g. retail and corporate customers, settlement institutions, service providers);
(f) Affected systems and technical details of the incident (e.g. source IP address and post, IOCs, tactics, techniques, procedures (TTPs));
(g) Root cause analysis; and
(h) Actions taken
- Escalation steps taken.
- Stakeholders informed.
- Response and recovery activities.
- Lessons learnt.

OM-5.5.61 **The penetration testing report as per Paragraph OM-5.5.28, along with the steps taken to mitigate the risks must be maintained by the licensee for a five year period from the date of the report and must be provided to CBB within two months following the end of the month where the testing took place, i.e. for a June test, the report must be submitted at the latest by 31st August and for a December test, by 28th February.**

OM-6.1 General Requirements

OM-6.1.1 **The requirements in Section OM-6.1 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-6.1 also apply to overseas Islamic bank licensees, but only with respect to the business booked in their branch in Bahrain.**

OM-6.1.2 **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-6.1.3 OM-6.1.2 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-6.1.4 **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-6.1.5 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-6.1.6 Translations produced in compliance with Rule OM-6.1.5 may be undertaken in-house, by an employee or contractor of the licensee, provided they are certified by an appropriate officer of the licensee.

MODULE	OM:	Operational Risk Management
CHAPTER	OM-6:	Books and Records

OM-6.1 General Requirements (continued)

OM-6.1.7 **Records must be accessible at any time from within the Kingdom of Bahrain, or as otherwise agreed with the CBB in writing.**

OM-6.1.8 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-6.1.9 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-6.1.10 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-6.1.11 **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.**

MODULE	OM:	Operational Risk Management
CHAPTER	OM-6:	Books and Records

OM-6.2 Transaction Records

OM-6.2.1 **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. (54) of 2018 with respect to Electronic Transactions "The Electronic Communications and Transactions Law" and its amendments.**

OM-6.2.2 **Rule OM-6.2.1 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-6.2.3 In the case of overseas Islamic bank licensees, Rule OM-6.2.1 therefore only applies to business booked in the Bahrain branch, not in the rest of the company.

OM-6.3 Other Records

Corporate Records

OM-6.3.1 **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-6.3.2 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-6 are limited to the business booked in their branch in Bahrain and the records of that branch (see Rule OM-6.1.1). They are thus not required to hold copies of shareholders' and Directors' meetings, except where relevant to the branch's operations.

Customer Records

OM-6.3.3 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-6.3.4 **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.**

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 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.

Appendix C – Cyber Security Control Guidelines

The Control Guidelines consists of five Core tasks which are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cyber security risk.

Identify – Develop a bank-wide understanding to manage cyber security risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Cyber Security Risk Management Framework. Understanding the business context, the resources that support critical functions, and the related cyber security risks enables a bank to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cyber security incident.

Detect – Develop and implement appropriate activities to identify the occurrence of a cyber security incident. The Detect Function enables timely discovery of cyber security events.

Respond – Develop and implement appropriate activities to take action regarding a detected cyber security incident. The Respond Function supports the ability to contain the impact of a potential cyber security incident.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cyber security incident.

Below is a listing of the specific cyber security activities that are common across all critical infrastructure sectors:

IDENTIFY

Asset Management: The data, personnel, devices, systems, and facilities that enable the bank to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the bank's risk strategy.

1. Physical devices and systems within the bank are inventoried.
2. Software platforms and applications within the bank are inventoried.
3. Communication and data flows are mapped.
4. External information systems are catalogued.
5. Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
6. Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

Business Environment: The bank's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities, and risk management decisions.

1. Priorities for the bank's mission, objectives, and activities are established and communicated.
2. Dependencies and critical functions for delivery of critical services are established.
3. Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).

Governance: The policies, procedures, and processes to manage and monitor the bank's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber security risk.

1. Bank's cyber security policy is established and communicated.
2. Cyber security roles and responsibilities are coordinated and aligned with internal roles and external partners.
3. Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, are understood and managed.
4. Governance and risk management processes address cyber security risks.

Risk Assessment: The bank understands the cyber security risk to bank's operations (including mission, functions, image, or reputation), bank's assets, and individuals.

1. Asset vulnerabilities are identified and documented.
2. Cyber threat intelligence is received from information sharing forums and sources.
3. Threats, both internal and external, are identified and documented.
4. Potential business impacts and likelihoods are identified.
5. Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
6. Risk responses are identified and prioritized.

Risk Management Strategy: The bank's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

1. Risk management processes are established, managed, and agreed to by bank's stakeholders.
2. The bank's risk tolerance is determined and clearly expressed.
3. The bank's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

Third Party Risk Management: The bank's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing third party risk. The bank has established and implemented the processes to identify, assess and manage supply chain risks.

1. Cyber third-party risk management processes are identified, established, assessed, managed, and agreed to by the bank's stakeholders.
2. Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber third-party risk assessment process.
3. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of a bank's cyber security program.
4. Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
5. Response and recovery planning and testing are conducted with suppliers and third-party providers.

PROTECT

Identity Management, Authentication and Access Control: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

1. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
2. Physical access to assets is managed and protected.
3. Remote access is managed.
4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
5. Network integrity is protected (e.g., network segregation, network segmentation).
6. Identities are proofed and bound to credentials and asserted in interactions
7. Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

Awareness and Training: The bank's personnel and partners are provided cyber security awareness education and are trained to perform their cyber security-related duties and responsibilities consistent with related policies, procedures, and agreements.

1. All users are informed and trained on a regular basis.
2. Bank's security awareness programs are updated at least annually to address new technologies, threats, standards, and business requirements.
3. Privileged users understand their roles and responsibilities.
4. Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
5. The Board and senior management understand their roles and responsibilities.
6. Physical and cyber security personnel understand their roles and responsibilities.
7. Software development personnel receive training in writing secure code for their specific development environment and responsibilities.

Data Security: Information and records (data) are managed consistent with the bank's risk strategy to protect the confidentiality, integrity, and availability of information.

1. Data-at-rest classified as critical or confidential is protected through strong encryption.
2. Data-in-transit classified as critical or confidential is protected through strong encryption.
3. Assets are formally managed throughout removal, transfers, and disposition
4. Adequate capacity to ensure availability is maintained.
5. Protections against data leaks are implemented.
6. Integrity checking mechanisms are used to verify software, firmware, and information integrity.
7. The development and testing environment(s) are separate from the production environment.
8. Integrity checking mechanisms are used to verify hardware integrity.

Information Protection Processes and Procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational units), processes, and procedures are maintained and used to manage protection of information systems and assets.

1. A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
2. A System Development Life Cycle to manage systems is implemented
3. Configuration change control processes are in place.
4. Backups of information are conducted, maintained, and tested.
5. Policy and regulations regarding the physical operating environment for bank's assets are met.
6. Data is destroyed according to policy.
7. Protection processes are improved.
8. Effectiveness of protection technologies is shared.
9. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
10. Response and recovery plans are tested.
11. Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening).
12. A vulnerability management plan is developed and implemented.

Maintenance: Maintenance and repairs of information system components are performed consistent with policies and procedures.

1. Maintenance and repair of bank's assets are performed and logged, with approved and controlled tools.
2. Remote maintenance of bank's assets is approved, logged, and performed in a manner that prevents unauthorized access.

Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
2. Removable media is protected and its use restricted according to policy.
3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
4. Communications and control networks are protected.
5. Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

DETECT

Anomalies and Events: Anomalous activity is detected and the potential impact of events is understood.

1. A baseline of network operations and expected data flows for users and systems is established and managed.
2. Detected events are analyzed to understand attack targets and methods.
3. Event data are collected and correlated from multiple sources and sensors
4. Impact of events is determined.
5. Incident alert thresholds are established.

Security Continuous Monitoring: The information system and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.

1. The network is monitored to detect potential cyber security events.
2. The physical environment is monitored to detect potential cyber security events
3. Personnel activity is monitored to detect potential cyber security events.
4. Malicious code is detected.
5. Unauthorized mobile code is detected.
6. External service provider activity is monitored to detect potential cyber security events.
7. Monitoring for unauthorized personnel, connections, devices, and software is performed.
8. Vulnerability scans are performed at least quarterly.

Detection Processes: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

1. Roles and responsibilities for detection are well defined to ensure accountability.
2. Detection activities comply with all applicable requirements.
3. Detection processes are tested.
4. Event detection information is communicated.
5. Detection processes are continuously improved.

RESPOND

Response Planning: Response processes and procedures are executed and maintained, to ensure response to detected cyber security incidents. Response plan is executed during or after an incident.

Communications: Response activities are coordinated with internal and external stakeholders.

1. Personnel know their roles and order of operations when a response is needed.
2. Incidents are reported consistent with established criteria.
3. Information is shared consistent with response plans.
4. Coordination with internal and external stakeholders occurs consistent with response plans.
5. Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness.
6. Incident response exercises and scenarios across departments are conducted at least annually.

Analysis: Analysis is conducted to ensure effective response and support recovery activities.

1. Notifications from detection systems are investigated.
2. The impact of the incident is understood.
3. Forensics are performed.
4. Incidents are categorized consistent with response plans.
5. Processes are established to receive, analyze and respond to vulnerabilities disclosed to the bank from internal and external sources (e.g. internal testing, security bulletins, or security researchers).

Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

1. Incidents are contained.
2. Incidents are mitigated.
3. Newly identified vulnerabilities are mitigated or documented as accepted risks.

Improvements: The response activities are improved by incorporating lessons learned from current and previous detection/response activities.

1. Response plans incorporate lessons learned.
2. Response strategies are updated.

RECOVER

Recovery Planning: Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cyber security incidents. Recovery plan is executed during or after a cyber security incident.

Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.

1. Recovery plans incorporate lessons learned.
2. Recovery strategies are updated.

Communications: Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

1. Public relations are managed.
2. Reputation is repaired after an incident.
3. Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.