FINANCING COMPANIES OPERATIONAL RISK MANAGEMENT MODULE

MODULE	OM Operational Risk Management
	Table of Contents

MODULE	OM Operational Risk Management
	Table of Contents

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 for financing company licensees operating in Bahrain on establishing parameters and control procedures to monitor and mitigate operational risks.

OM-A.1.2 This Module provides support for certain other parts of the Rulebook, mainly:
(a) Principles of Business; and
(b) High-level Controls.

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 financing company 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 January 2014 by the CBB. 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 most recent changes made to this Module are detailed in the table below:

Summary of Changes

Module Ref.	Change Date	Description of Changes
OM-2.9	07/2016	Added new Section dealing with outsourcing of functions containing customer information.
OM-4.9	10/2016	Added new Section on Cyber Security Risk Management
OM-5.3	10/2016	Added new Section on Cyber Security Measures
OM-2.9.2	01/2017	Amended Paragraph on customer information
OM-5.1.19 & OM-5.1.19A	01/2017	Added Paragraphs on PCI-DSS certification.
OM-5.1.20	04/2017	Added a Paragraph on Geolocation Limitation
OM-5.1.20A	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-5.1.20B	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-5.1.20C	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-5.1.20D	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-5.1.20E	07/2017	Added new paragraph on Prohibition of Double Swiping.
OM-2.1.2	10/2017	Amended Paragraph on outsourcing, to allow the utilization of cloud services and customer call centres.
OM-2.1.4	10/2017	Added a new Paragraph on outsourcing.
OM-2.1.5	10/2017	Added a new Paragraph on outsourcing.
OM-2.3.1	10/2017	Amended Paragraph.
OM-2.3.6	10/2017	Amended Paragraph.
OM-2.3.7	10/2017	Amended Paragraph.
OM-2.4.2	10/2017	Amended Paragraph.
OM-2.4.3	10/2017	Deleted Paragraph.
OM-2.4.5	10/2017	Amended Paragraph.
OM-2.5.1(a)	10/2017	Amended sub-sub-paragraph no. (5).
OM-2.5.1(c)	10/2017	Amended sub-sub-paragraphs no. (2) and (3).
OM-2.5.1(e)	10/2017	Amended sub-sub-paragraph no. (3).
OM-2.8.3	10/2017	Amended Paragraph.
OM-2.9.1	10/2017	Amended Paragraph.
OM-2.9.4(b)	10/2017	Amended sub-paragraph.
OM-2.9.4(c)	10/2017	Amended sub-paragraph.
OM-2.9.4(d)	10/2017	Deleted sub-paragraph.
OM-2.9.5	10/2017	Deleted paragraph.
OM-2.9.6	10/2017	Added a new paragraph for security measures related to cloud services.
OM-5.1.20AA	04/2018	Added a new Paragraph on card (EMV) compliance.
OM-5.1.20BB	04/2018	Added a new Paragraph on provision of cash withdrawal and payment services through various channels.
OM-2.9.2	07/2018	Amended Paragraph to include call centres.
OM-2.9.2A	07/2018	Added new Paragraph on customer notification.
OM-5.1.21 & OM-5.1.22	10/2019	Added new Paragraphs on Contactless Payment Transactions.

OM-A.2 Module History Contd.

Summary of Changes

Module Ref.	Change Date	Description of Changes

Superseded Requirements

OM-A.2.3 This Module supersedes the following provisions contained in circulars or other regulatory requirements:

Document Ref.	Document Subject
Volumes 1 and 2	Module OM
EDBS/KH/C/33/2018	Amendments to the Operational Risk Management Module

OM-B.1 Scope

OM-B.1.1 This Module applies to all financing company licensees authorised in the Kingdom, thereafter referred to in this Module as licensees.

OM-1.1 Overview

OM-1.1.1 This Module provides guidance and rules for operational risk and sets out requirements for an appropriate risk management environment, including outsourcing, electronic financing activities, business continuity and security measures.

OM-1.1.2 Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk[1], but excludes strategic and reputational risk.

OM-1.1.3 Operational risk is inherent in all types of licensees' transactions and activities, processes and systems, and the effective management of operational risk must be a fundamental element of a licensee's risk management programme. Sound operational risk governance relies upon three lines of defence:

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

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

OM-1.2 Developing an Appropriate Risk Management Environment

OM-1.2.1 **Licensee's management must implement policies and procedures to manage risks arising out of a licensee's activities. The licensee must maintain written policies and procedures that identify the risk tolerances approved by the Board of Directors and must clearly delineate lines of authority and responsibility for managing the risks. Licensees' employees and credit officers in particular must be fully aware of all policies and procedures that relate to their specific duties.**

OM-1.2.2 **The board of directors must take the lead in establishing a strong risk management culture. The board of directors and senior management must establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.**

OM-1.2.3 **The operational risk management function must be functionally independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk framework within the licensee.**

OM-1.2.4 For the purpose of Paragraph OM-1.2.3, 'functionally independent' means that the risk management function cannot report hierarchically and/or functionally to any person or function that is directly responsible for risk generation.

OM-1.2.5 The operational risk management function should include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the operational risk management function is to challenge the business lines' inputs to, and outputs from, the licensee's risk management, risk measurement and reporting systems. The operational risk management function should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.

OM-1.2.6 Both the board and senior management are responsible for creating an organisational culture that places high priority on effective operational risk management and adherence to sound operating controls. Operational risk management is most effective where a licensee's culture emphasises high standards of ethical behaviour at all levels of the licensee. The board and senior management should promote an organisational culture which establishes through both actions and words the expectations of integrity for all employees in conducting the business of the licensee.

OM-1.2 Developing an Appropriate Risk Management Environment (continued)

The Board of Directors

OM-1.2.7 The board of directors must establish, approve and periodically review the framework. The board of directors must oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

OM-1.2.8 The board of directors must:

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

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

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

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

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

OM-1.2.9 Strong internal controls are a critical aspect of operational risk management, and the board of directors must establish clear lines of management responsibility and accountability for implementing a strong control environment. The control environment must provide appropriate independence/separation of duties between operational risk management functions, business lines and support functions

OM-1.2 Developing an Appropriate Risk Management Environment (continued)

The Role of Committees

OM-1.2.10 A licensee's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, a licensee must take the following into consideration:
(a) Committee structure;
(b) Committee composition; and
(c) Committee operation.

OM-1.2.11 Sound industry practice for larger and more complex organisations with a central group function and separate business units is to utilise a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports. Depending on the nature, size and complexity of the licensee, the enterprise level risk committee may receive input from operational risk committees by country, business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board's risk management committee.

OM-1.2.12 Sound industry practice is for operational risk committees (or the risk committee in smaller licensees) to include a combination of members with expertise in business activities and financial, as well as independent risk management

Risk Appetite and Tolerance

OM-1.2.13 **The board of directors must approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk that the licensee is willing to assume.**

OM-1.2.14 **When approving and reviewing the risk appetite and tolerance statement, the board of directors must consider all relevant risks, the licensee's level of risk aversion, its current financial condition and the licensee's strategic direction. The board of directors must approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite and tolerance.**

OM-1.2.15 The risk appetite and tolerance statement should encapsulate the various operational risk appetites within a licensee and ensure that they are consistent.

OM-1.2 Developing an Appropriate Risk Management Environment (continued)

OM-1.2.16 **The board of directors must regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statement. This review must consider changes in the external environment, material increases in business or activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume or nature of limit breaches. The board must monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.**

OM-1.2.17 **The licensee must ensure that the internal pricing and performance measurement mechanisms appropriately take into account operational risk. Where operational risk is not considered, risk-taking incentives might not be appropriately aligned with the risk appetite and tolerance.**

Ethics Policy

OM-1.2.18 **The board of directors must establish a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts (See Section HC-2.2).**

OM-1.2.19 Clear expectations and accountabilities ensure that staff understand their roles and responsibilities for risk, as well as their authority to act. Strong and consistent senior management support for risk management and ethical behaviour convincingly reinforces codes of conduct and ethics, compensation strategies, and training programmes.

Compensation Policies

OM-1.2.20 **Compensation policies must be aligned to the licensee's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They must also appropriately balance risk and reward.**

Operational Risk Training

OM-1.2.21 Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organisation. Training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.

OM-1.2 Developing an Appropriate Risk Management Environment (continued)

Risk Management Framework

OM-1.2.22 **Licensees must develop, implement and maintain a framework that is fully integrated into the licensee's overall risk management processes.**

OM-1.2.23 The framework for operational risk management chosen by an individual licensee will depend on a range of factors, including its nature, size, complexity and risk profile.

OM-1.2.24 The board is responsible for establishing a management structure capable of implementing the licensee's operational risk management framework. Since a significant aspect of managing operational risk relates to the establishment of strong internal controls, it is particularly important that the board establishes clear lines of management responsibility, accountability and reporting. In addition, there should be separation of responsibilities and reporting lines between operational risk control functions, business lines and support functions in order to avoid conflicts of interest. The framework should also articulate the key processes the licensee needs to have in place to manage operational risk.

OM-1.2.25 **The framework must be comprehensively and appropriately documented in board of directors approved policies and must include definitions of operational risk and operational loss.**

OM-1.2.26 Licensees that do not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of their framework.

OM-1.2.27 **Framework documentation must clearly:**

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

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

(c) Describe the licensee's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;

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

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

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

OM-1.2 Developing an Appropriate Risk Management Environment (continued)

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

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

OM-1.2.28 The board should review the framework regularly to ensure that the licensee is managing the operational risks arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities or systems. This review process should also aim to assess industry best practice in operational risk management appropriate for the licensee's activities, systems and processes. If necessary, the board should ensure that the operational risk management framework is revised in light of this analysis, so that material operational risks are captured within the framework.

Independent Review of Operational Risk

OM-1.2.29 **The board of directors must ensure that the licensee's operational risk management framework is subject to effective and comprehensive independent review.**

OM-1.2.30 **The independent review functions are the internal audit and compliance functions and the staff occupying these functions must be competent and appropriately trained and not be involved in the development, implementation and operation of the operational risk framework.**

OM-1.2.31 With reference to Paragraph OM-1.2.30, internal audit and compliance should not be involved with the setting of risk appetite or risk tolerance. Internal audit should be reviewing the robustness of the process of how these limits are set and why and how they are adjusted in response to changing circumstances. More details on the internal audit function and the role of the audit committee are included in Chapter HC-3.

OM-1.2.32 An independent review consists of the verification of the framework on a periodic basis and is typically performed by the licensee's internal and/or external audit, but may involve other suitably qualified independent parties from external sources. Verification activities test the effectiveness of the overall framework, consistent with policies approved by the board of directors, and also test validation processes to ensure that they are independent and implemented in a manner consistent with established policies of the licensee.

OM-1.2 Developing an Appropriate Risk Management Environment (continued)

OM-1.2.33 Licensees should have in place adequate internal audit coverage to verify that operating policies and procedures have been implemented effectively. The board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the audit programme is appropriate to the risk exposures. Audit should periodically validate that the licensee's operational risk management framework is being implemented effectively across the licensee.

Senior Management

OM-1.2.34 **The responsibilities of the senior management of the licensee must include:**

(a) Developing for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility;

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

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

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

(e) Developing, maintaining and implementing policies, processes and procedures for managing operational risk in all of the licensee's products, activities, processes and systems consistent with the risk appetite and tolerance;

(f) Developing succession plans for senior staff; and

(g) Developing business continuity plans for the licensee.

OM-1.2.35 **Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. These must include systems to report, track and, when necessary, escalate issues to ensure resolution. Licensees must be able to demonstrate that the three lines of defence 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 Developing an Appropriate Risk Management Environment (continued)

OM-1.2.36 **Senior management must translate the operational risk strategy established by the board of directors into an operational risk management framework that refers to specific policies, processes and procedures that can be implemented and verified within the different business units.**

OM-1.2.37 While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures and controls within its purview, senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability.

OM-1.2.38 **Senior management must ensure that the necessary resources are available to manage operational risk effectively. Moreover, senior management must assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's activity.**

OM-1.2.39 Senior management should ensure that the licensee's activities are conducted by qualified staff with the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should have authority independent from the units they oversee.

OM-1.2.40 **Senior management must ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the licensee who are responsible for the procurement of external services such as insurance purchasing and outsourcing agreements. Failure to do so could result in significant gaps or overlaps in a licensee's overall risk management programme.**

OM-1.2.41 The managers of the corporate operational risk management function should be of sufficient stature within the licensee to perform their duties effectively, ideally evidenced by title commensurate with other risk management functions such as credit, market and liquidity risk.

OM-1.2.42 Particular attention should be given to the quality of documentation controls and to transaction-handling practices. Policies, processes and procedures related to advanced technologies supporting high transactions volumes, in particular, should be well documented and disseminated to all relevant personnel.

OM-1.2 Developing an Appropriate Risk Management Environment (continued)

Management Information System

OM-1.2.43 The management information system of an organisation plays a key role in establishing and maintaining an effective operational risk management framework.

OM-1.2.44 Communication flow serves the purpose of establishing a consistent operational risk management culture across the licensee. Reporting flow enables:

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

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

OM-1.3 Identification and Assessment

OM-1.3.1 **Licensees must identify and assess the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood. Licensees must also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.**

OM-1.3.2 Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal factors (such as the licensee's structure, the nature of the licensee's activities, the quality of the licensee's human resources, organisational changes and employee turnover) and external factors (such as changes in the broader environment and the industry and technological advances) that could adversely affect the achievement of the licensee's objectives.

OM-1.3.3 In addition to identifying the most potentially adverse risks, licensees should assess their vulnerability to these risks. Sound risk assessment allows the licensee to better understand its risk profile and most effectively target risk management resources.

OM-1.3.4 Amongst the possible tools used by licensees for identifying and assessing operational risk are:

(a) Self- or Risk Assessment: a licensee assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment. Scorecards, for example, provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address inherent risks, as well as the controls to mitigate them;

(b) Risk Mapping: in this process, various business units, organisational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action;

(c) Risk Indicators: risk indicators are statistics and/or metrics, often financial, which can provide insight into a licensee's risk position. These indicators tend to be reviewed on a periodic basis (such as monthly or quarterly) to alert licensees to changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions; and

OM-1.3 Identification and Assessment (continued)

(d) Measurement: some licensees have begun to quantify their exposure to operational risk using a variety of approaches. For example, data on a licensee's historical loss experience could provide meaningful information for assessing the licensee's exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events. Some licensees have also combined internal loss data with external loss data, scenario analyses, and risk assessment factors.

Approval Process

OM-1.3.5 **Senior management must ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.**

OM-1.3.6 In general, a licensee's operational risk exposure is increased when a licensee engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Moreover, the level of risk may escalate when new products activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business-critical operations. A licensee should ensure that its risk management control infrastructure is appropriate at inception and that it keeps pace with the rate of growth of, or changes to, products activities, processes and systems.

OM-1.3.7 **A licensee must have policies and procedures that address the process for review and approval of new products, activities, processes and systems.**

OM-1.3.8 The review and approval process referred to in Paragraph OM-1.3.7 should consider:

(a) Inherent risks in the new product, service, or activity;
(b) Changes to the licensee's operational risk profile and appetite and tolerance, including the risk of existing products or activities;
(c) The necessary controls, risk management processes, and risk mitigation strategies;
(d) The residual risk;
(e) Changes to relevant risk thresholds or limits; and
(f) The procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

OM-1.3 Identification and Assessment (continued)

OM-1.3.9 The approval process should also ensure that appropriate investment has been made for human resources and technology infrastructure before new products are introduced. The implementation of new products, activities, processes and systems should be monitored in order to identify any material differences to the expected operational risk profile, and to manage any unexpected risks.

OM-1.4 Monitoring

OM-1.4.1 **Licensees must implement a process to regularly monitor operational risk profiles and material exposures to losses. There must be regular reporting of pertinent information at the board, senior management and business levels that supports the proactive management of operational risk.**

OM-1.4.2 Licensees are encouraged to continuously improve the quality of operational risk reporting. A licensee should ensure that its reports are comprehensive, accurate, consistent and actionable across business lines and products. Reports should be manageable in scope and volume; effective decision-making is impeded by both excessive amounts and paucity of data.

OM-1.4.3 Reporting should be timely and a licensee should be able to produce reports in both normal and stressed market conditions. The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring should be an integrated part of a licensee's activities. The results of these monitoring activities should be included in regular management and board reports, as should compliance reviews performed by the internal audit and/or risk management functions. Reports generated by (and/or for) supervisory authorities may also inform this monitoring and should likewise be reported internally to senior management and the board, where appropriate.

OM-1.4.4 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 licensee'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 licensee.

OM-1.4.5 Data capture and risk reporting processes should be analysed periodically with a view to continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.

OM-1.5 Control and Mitigation

OM-1.5.1 **Licensees must have a strong control environment that utilises:**

(a) Policies, processes and systems;
(b) Appropriate internal controls; and
(c) Appropriate risk mitigation and/or transfer strategies.

OM-1.5.2 **Internal controls must be designed to provide assurance that a licensee will:**

(a) Have efficient and effective operations;
(b) Safeguard its assets;
(c) Produce reliable financial reports; and
(d) Comply with applicable laws and regulations.

OM-1.5.3 Control activities are designed to address the operational risks that a licensee has identified. For all material operational risks that have been identified, the licensee should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, the licensee should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

OM-1.5.4 Control processes and procedures should be established and licensees 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 licensee's progress towards the stated objectives;
(b) Verifying compliance with management controls;
(c) Policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues;
(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-1.5.5 Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. Both the board of directors and senior management are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of a licensee. Controls that are an integral part of the regular activities enable quick responses to changing conditions and avoid unnecessary costs.

OM-1.5 Control and Mitigation (continued)

OM-1.5.6 An effective internal control system also requires that there be appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to individuals, or a team, may enable them to conceal losses, errors or inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimised, and subject to careful independent monitoring and review.

OM-1.5.7 In addition to segregation of duties, licensees should ensure that other internal practices are in place as appropriate to control operational risk. Examples of these include:

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

OM-1.5.8 Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or programmes can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalise the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

OM-1.5.9 Licensees should view risk mitigation tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly recognise and rectify legitimate 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, or transfer the risk to another business sector or area, or even create a new risk (e.g. legal or counterparty risk).

OM-1.5.10 Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, licensees should be aware that increased automation could transform high-frequency, low-severity losses into low frequency, high-severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by factors beyond the licensee's immediate control (e.g., external events). Such problems may cause serious difficulties for licensees and could jeopardise an institution's ability to conduct key business activities.

OM-1.5 Control and Mitigation (continued)

OM-1.5.11 In some instances, licensees may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organisation and should be consistent with the licensee's overall business strategy and appetite for risk.

OM-1.5.12 Licensees should assess the costs and benefits of alternative risk limitation and control strategies and should adjust their operational risk exposure using appropriate strategies, in light of their overall risk profile.

OM-1.6 Succession Planning

OM-1.6.1 Succession planning is an essential precautionary measure for a licensee 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-1.6.2 **The CBB requires licensees to document succession plans for their senior management team and have these ready at any time for onsite inspection by CBB staff. Licensees must summarise who is covered by their succession plan and confirm that the plan has been reviewed and endorsed at Board level.**

OM-1.7 Disclosure

OM-1.7.1 **A licensee's public disclosures must allow stakeholders to assess its approach to operational risk management.**

OM-1.7.2 A licensee'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 licensee's operations, and evolving industry practice. See Section PD-1.3 on disclosure requirements.

OM-1.7.3 A licensee should disclose its operational risk management framework in a manner that will allow stakeholders to determine whether the licensee identifies, assesses, monitors and controls/mitigates operational risk effectively.

OM-1.7.4 A licensee's disclosures should be consistent with how senior management and the board of directors assess and manage the operational risk of the licensee.

OM-1.7.5 **A licensee must have a formal disclosure policy approved by the board of directors that addresses the licensee's approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, licensees must implement a process for assessing the appropriateness of their disclosures, including the verification and frequency of them.**

MODULE	OM:	Operational Risk Management
CHAPTER	OM-2:	Outsourcing

OM-2.1 Introduction

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 would normally be undertaken by the licensee itself (or in the case of a new activity, one which commonly would have been performed internally by the licensee) as part of the offering of regulated financial services. Examples of services that are sometimes outsourced include data processing, cloud services, customer call centres and back-office related activities.**

OM-2.1.3 Most of the Directives in this Chapter are concerned with situations where the third party provider is outside the licensee. Section OM-2.8, however, sets out the CBB's requirements when a service is outsourced to a company within the licensee's group.

OM-2.1.4 For outsourcing services that are not considered material outsourcing arrangements, licensees must submit a written notification to the CBB before committing to the new outsourcing arrangement.

OM-2.1.5 The CBB reserves the right to require a licensee to terminate or make alternative outsourcing arrangements if, among other reasons, the confidentiality of its customer information was, or is likely to be, breached or the ability of the CBB to carry out its supervisory functions in view of the outsourcing arrangement cannot be assured or executed.

OM-2.2 Supervisory Approach

OM-2.2.1 The CBB recognises the benefits that can potentially be achieved through outsourcing an activity to a third party provider. They can include reduced costs, enhanced service quality and a reduction in management time spent on non-core activities. However, outsourcing an activity also poses potential risks. These include the ability of the service provider to maintain service quality levels, reduced control over the activity and access to relevant information, and increased legal and client confidentiality risks.

OM-2.2.2 **The CBB's approach is to allow licensees the freedom to enter into outsourcing arrangements, providing these are not core functions and these arrangements have been properly structured and associated risks addressed.**

OM-2.2.3 **Once an outsourcing arrangement has been implemented, the CBB requires a licensee to continue to monitor the associated risks and the effectiveness of its mitigating controls. It will verify this through the course of its normal on-site and off-site supervisory processes, such as prudential meetings and on-site examinations. The CBB also requires access to the outsourced activity, which it may occasionally want to examine itself, through management meetings or on-site examinations.**

OM-2.2.4 **Fundamental to the CBB's supervisory approach to outsourcing is that the Board and management of the licensee may not abdicate their responsibility for a licensee's business and the way its customers are treated. The Board and management remain ultimately responsible for the effectiveness of systems and controls in outsourced activities.**

OM-2.2 Supervisory Approach (continued)

OM-2.2.5 The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass:

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

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

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

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

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

(f) Development of viable contingency plans; and

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

OM-2.3 Prior Approval Requirements

OM-2.3.1 **A licensee must seek the CBB's prior written approval before committing to a new outsourcing arrangement.**

OM-2.3.2 **The request for prior approval must:**

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

(b) Contain sufficient detail to demonstrate that relevant issues raised in Section OM-2.4 onward of this Chapter have been addressed; and

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

OM-2.3.3 **Licensees must not outsource "core functions" which are defined as the offering of regulated financing company services, customer due diligence and approval of customers. Core functions also include arrangements that, if they failed in any way, would pose significant risks to the on-going operations of a licensee, its reputation and/or quality of service provided to its customers.**

OM-2.3.4 With reference to Paragraph OM-2.3.3, the outsourcing of all or a substantial part of functions such as loan processing and settlements would normally be considered 'core'. IT and data processing may be considered 'non-core' and may be outsourced subject to the CBB prior approval.

OM-2.3.5 Management should carefully consider whether a proposed outsourcing arrangement falls under this Chapter's definition of 'core'. If in doubt, management should consult with the CBB.

OM-2.3.6 The CBB will review the information provided and provide a definitive response within 6 weeks of receiving the request for approval. Where further information is requested from the licensee, however, the time taken to provide this further information will not be taken into account.

OM-2.3.7 **Once an activity has been outsourced, a licensee must immediately inform its normal supervisory point of contact at the CBB of any material problems encountered with the outsourcing provider. The CBB reserves the right to direct a licensee to make alternative arrangements for the outsourced activity.**

OM-2.4 Risk Assessment

OM-2.4.1 **Licensees must undertake a thorough risk assessment of an outsourcing proposal, before formally submitting a request for prior approval to the CBB and committing itself to an agreement.**

OM-2.4.2 **The risk assessment must – amongst other things – include an analysis of:**

(a) The business case;

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

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

OM-2.4.3 [This paragraph was deleted in October 2017].

OM-2.4.4 **Once an outsourcing agreement has been entered into, licensees must regularly review the suitability of the outsourcing provider and the on-going impact of the agreement on their risk profile and systems and controls framework. Such reviews must take place at least every year.**

OM-2.4.5 **A licensee must nominate a relevant approved person with day-to-day responsibility for handling the relationship with the outsourcing provider and ensuring that relevant risks are addressed. The name of this person must be communicated to the CBB as part of the request for prior approval ~~process~~ required under Section OM-2.3 or if any change occurs thereafter. Any subsequent replacement of such person must also be notified to the CBB.**

OM-2.5 Outsourcing Agreement

OM-2.5.1 The activities to be outsourced and respective contractual liabilities and obligations of the outsourcing provider and licensee must be clearly specified in an outsourcing agreement. This agreement must – amongst other things – address the following points:

(a) Control over outsourced activities:

(i) The Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls over the outsourced activities. Licensees must therefore ensure that they have adequate mechanisms for monitoring the performance of, and managing the relationship with, the outsourcing provider;

(ii) A service level agreement ("SLA") – setting out the standards of service to be provided – must form part of the outsourcing agreement;

(iii) Mechanisms for the regular monitoring by licensees of performance against the SLA and other targets, and for implementing remedies in case of any shortfalls, must also form part of the agreement;

(iv) Clear reporting and escalation mechanisms must be specified in the agreement; and

(v) Where an outsourcing provider in turn decides to sub-contract to other providers, CBB's prior written approval must be obtained, and it must obtain the prior consent of the concerned licensee before sub-contracting and the original provider must remain contractually liable to the licensee for the quality and level of service agreed, and its obligations to the licensee must remain unchanged;

OM-2.5 Outsourcing Agreement (continued)

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

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

OM-2.5 Outsourcing Agreement (continued)

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

(d) Business continuity:

(i) Licensees must ensure that service providers maintain, regularly review and test plans to ensure continuity in the provision of the outsourced service; and

(ii) Licensees must have an adequate understanding of the outsourcing provider's arrangements, to understand the implications for its own contingency arrangements (see Section OM-2.6);

(e) Termination:

(i) Licensees must have the right to terminate the agreement should the outsourcing provider undergo a change of ownership (whether direct or indirect) that poses a potential conflict of interest; becomes insolvent; or goes into liquidation or administration;

(ii) Termination under any other circumstances allowed under the agreement must give licensees a sufficient notice period in which they can effect a smooth transfer of the service to another provider or bring it back in-house; and

(iii) In the event of termination, for whatever reason, the agreement must provide for the return of all customer data – where required by licensees – or destruction of the records.

OM-2.6 Contingency Planning for Outsourcing Arrangements

OM-2.6.1 Licensees must maintain and regularly review contingency plans to enable them to set up alternative arrangements – with minimum disruption to business – should the outsourcing contract be suddenly terminated or the outsourcing provider fails. This may involve the identification of alternative outsourcing providers or the provision of the service in-house. These plans must consider how long the transition would take and what interim arrangements would apply.

OM-2.7 Internal Audit Outsourcing

OM-2.7.1 Because of the critical importance of an effective internal audit function to a licensee's control framework, all proposals to outsource internal audit operations are subject to CBB prior approval.

OM-2.7.2 Licensees must not outsource their internal audit function to the same firm that acts as their external auditor.

OM-2.7.3 In all circumstances, Board and management of licensees must retain responsibility for ensuring that an adequate internal audit programme is implemented, and will be held accountable in this respect by the CBB.

OM-2.8 Intragroup Outsourcing

OM-2.8.1 **As with outsourcing to non-group companies, the Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in activities outsourced to group companies.**

OM-2.8.2 However, the degree of formality required – in terms of contractual agreements and control mechanisms – for outsourcing within a licensee's group is likely to be less, because of common management and enhanced knowledge of other group companies.

OM-2.8.3 **A licensee must formally request prior written approval from the CBB at least 6 weeks before committing to an intragroup outsourcing. The request for approval must be made in writing to the licensee's normal supervisory point of contact, and must set out a summary of the proposed outsourcing, its rationale, and an analysis of its associated risks and proposed mitigating controls. The CBB will respond to the request for approval in the same manner and timescale as set in Section OM-2.3.**

OM-2.8.4 The CBB expects, as a minimum, an agreed statement of the standard of service to be provided by the group provider, including a clear statement of responsibilities allocated between the group provider and licensee.

OM-2.8.5 The CBB also expects a licensee's management to have addressed the issues of customer confidentiality, access to information and business continuity covered above (Section OM-2.5).

OM-2.9 Outsourcing of Functions Containing Customer Information

OM-2.9.1 Licensees must seek the CBB's prior written approval for third party and intragroup outsourcing of functions/services containing customer information including but not limited to payment services, debt collection, card and data processing, IT function including cloud services, internal audit and electronic/internet banking services but excluding legal services.

OM-2.9.2 For a third party outsourcing of functions/services containing customer information, other than debt collection, IT function, internal audit, cards embossing, data/documents storing and call centres, the service providers must be licensed by the CBB and located in Bahrain. If the outsourced service is not available in Bahrain after 30th June 2017, licensees must submit to the CBB a written request, at least within 30 days of the stated deadline. The request must provide details of the circumstances under which the extension of outsourcing activities is being requested.

OM-2.9.2A In case of an outsourcing arrangement that involves transmission of customer information to the service provider, licensees must make necessary changes to the terms of the customer agreements and send prior notices to the customer, who shall provide a consent in writing that his/her information would be transmitted to a service provider. Licensees may only effect the changes in the customer agreement following the receipt of customer consent.

OM-2.9.3 Licensees must provide to the CBB quarterly progress reports on the steps and procedures taken in implementing the requirements of Paragraph OM-2.9.2. The progress report must be provided to the licensee's supervisory point of contact at the CBB and the first report must be submitted by 31st July 2016.

OM-2.9 Outsourcing of Functions Containing Customer Information (continued)

OM-2.9.4 **For intragroup outsourcing of functions/services containing customer information, the following conditions must also be met:**

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

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

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

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

OM-2.9.5 **[This Paragraph was deleted in October 2017].**

Clouding Services

OM-2.9.6 **For the purpose of outsourcing of cloud services, licensees must ensure that, at a minimum, the following security measures are in place:**

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

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

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

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

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

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

OM-3.1 Electronic Financial Services

OM-3.1.1 As the Board of Directors and senior management should take an explicit, informed and documented strategic decision as to whether and how the licensee is to provide electronic financial services. The initial decision should include the specific accountabilities, policies and controls to address risks, including those arising in a cross-border context.

OM-3.1.2 Effective management oversight should include the review and approval of the key aspects of the licensee's security control process, such as the development and maintenance of a security control infrastructure that properly safeguards the electronic financial systems and data from both internal and external threats. The review should also include a comprehensive process for managing risks associated with increased complexity of and increasing reliance on outsourcing relationships and third-party dependencies to perform electronic financing functions.

OM-3.1.3 Senior management should ensure that appropriate security control processes are in place for electronic financing. Such processes should include establishing appropriate authorisation privileges and authentication measures, logical and physical access controls, adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities and data integrity of transactions, records and information.

OM-3.1.4 The existence of clear audit trails for all electronic financing transactions should be ensured and measures to preserve confidentiality of key electronic financing information should be appropriate with the sensitivity of such information.

OM-3.1.5 To protect licensees against business, legal and reputation risk, electronic financial services should be delivered on a consistent and timely basis in accordance with high customer expectations for constant and rapid availability and potentially high transaction demand. Licensees should have the ability to deliver electronic financing services to all end-users and be able to maintain such availability in all circumstances.

OM-3.1.6 Licensees should develop appropriate incident response plans, including communication strategies that ensure business continuity, control reputation risk and limit liability associated with disruptions in their electronic financing services.

MODULE	OM:	Operational Risk Management
CHAPTER	OM-4:	Business Continuity Planning

OM-4.1 General Requirements

OM-4.1.1 **To ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption, all licensees must maintain contingency and business continuity plan (BCP) to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption. 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; and
(f) Communications with and reporting to the CBB and any other relevant regulators.

OM-4.1.2 For reasons that may be beyond a licensee's control, a severe event may result in the inability of the licensee to fulfil some or all of its business obligations, particularly where the licensee's physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the licensee. This potential event requires that licensees establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the licensee may be vulnerable, commensurate with the size and complexity of the licensee's operations.

OM-4.1.3 Licensees should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. For these processes, licensees should identify alternative mechanisms for resuming service in the event of an outage. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption. Where such records are backed-up at an off-site facility, or where a licensee's operations must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimise the risk that both primary and back-up records and facilities will be unavailable simultaneously.

OM-4.1.4 Licensees should periodically review their disaster recovery and business continuity plans so that they are consistent with the licensee's current operations and business strategies. Moreover, these plans should be tested periodically to ensure that the licensee would be able to execute the plans in the unlikely event of a severe business disruption.

OM-4.1 General Requirements (continued)

OM-4.1.5 Effective BCPs must be comprehensive, limited not just to disruption of business premises and information technology facilities, but covering all other critical areas, which affect the continuity of critical business operations or services (e.g. liquidity, human resources and others).

OM-4.1.6 Licensees must notify the CBB promptly if their BCP is activated. They must also provide regular progress reports – as agreed with the CBB – until the BCP is deactivated.

OM-4.2 Board and Senior Management Responsibilities

Establishment of Policy, Processes & Responsibilities

OM-4.2.1 A licensee's Board of Directors and senior management are collectively responsible for a licensee's business continuity. The Board must endorse the policies, standards and processes for a licensee's BCP, as established by its senior management. The Board and senior management must delegate adequate resources to develop the BCP, and for its maintenance and periodic testing.

OM-4.2.2 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-4.2.3 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-4.2.4 The CMT must submit regular reports to the Board and senior management on the results of the testing of the BCP (refer to section OM-4.8). Major changes must be developed by the CMT, reported to senior management, and endorsed by the Board.

OM-4.2.5 The Chief Executive of a licensee must sign a formal annual statement submitted to the Board on whether the recovery strategies adopted are still valid and whether the documented BCP is properly tested and maintained. The annual statement must be included in the BCP documentation and will be reviewed as part of the CBB's on-site examinations.

OM-4.3 Developing a Business Continuity Plan

Impact Analysis

OM-4.3.1 **Licensees' BCPs must be based on:**
(a) A business impact analysis;
(b) An operational impact analysis; and
(c) A financial impact analysis.
These analyses must be comprehensive, including all business functions and departments, not just IT or data processing.

OM-4.3.2 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-4.3.3 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-4.3.4 Operational impact analysis focuses on the licensee's ability to maintain communications with customers and to retrieve key activity records. It identifies the organisational 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-4.3.5 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-4.3.6 **In developing a BCP, licensees must consider realistic threat scenarios that may (potentially) cause disruptions to their business processes.**

OM-4.3 Developing a Business Continuity Plan (continued)

OM-4.3.7 Business continuity plans must take into account different types of likely or plausible scenarios to which the licensee will be vulnerable. 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 BCP – Recovery Levels & Objectives

OM-4.4.1 **The BCP must document strategies and procedures to maintain, resume and recover critical business operations or services. The plan must differentiate between critical and non-critical functions. The BCP must clearly describe the types of events that would lead up to the formal declaration of a business disruption and the process for activating the BCP.**

OM-4.4.2 **The BCP must clearly identify alternate sites for different operations, the total number of recovery personnel, workspace requirements, and applications and technology requirements. Office facilities and records requirements must also be identified.**

OM-4.4.3 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.

OM-4.4.4 **Individual critical business and support functions must establish the minimum BCP recovery objectives for recovering essential business operations and supporting systems to a specified level of service ("recovery level") within a defined period following a disruption ("recovery time"). These recovery levels and recovery times must be approved by the senior management prior to proceeding to the development of the BCP.**

List of Contacts and Responsibilities

OM-4.4.5 **The BCP must contain a list of all key personnel. The list must include personal contact information on each key employee such as their home address, home telephone number, and cell phone so they may be contacted in case of a disaster or other emergency.**

OM-4.4 BCP – Recovery Levels & Objectives (continued)

OM-4.4.6 **The BCP must contain all the necessary process steps to complete each critical business operation or service. Each process must be explained in sufficient detail to allow another employee to perform the job in case of a disaster.**

Alternate Sites for Business and Technology Recovery

OM-4.4.7 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 premises owned or under the control of the licensee. A useable, functional alternate site is an integral component of BCP.

OM-4.4.8 **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-4.4.9 **Licensees' alternate sites and alternate recovery mechanisms 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 the licensee's security policy.**

OM-4.4.10 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-4.4 BCP – Recovery Levels & Objectives (continued)

OM-4.4.11 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-4.4.12 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-4.4.13 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-4.4.14 Certain licensees may rely on a reciprocal recovery arrangement with other institutions to provide recovery capability. 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-4.5 Detailed Procedures for the BCP

OM-4.5.1 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-4.5.2 **A BCP must set out a Crisis Management Plan (CMP) that serves as a documented guidance to assist the CMT in dealing with a crisis situation to avoid spill over effects to the business as a whole. The overall CMP, at a minimum, must contain the following:**

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

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

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

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

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

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

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

OM-4.5 Detailed Procedures for the BCP (continued)

OM-4.5.3 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-4.5.4 **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.**

Technology Recovery

OM-4.5.5 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-4.5.6 Licensees should pay attention to the resilience of critical technology equipment and facilities such as the uninterruptible power supply (UPS) and the computer cooling systems. Such equipment and facilities should be subject to continuous monitoring and periodic maintenance and testing.

OM-4.5.7 **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.**

OM-4.6 Vital Records Management

OM-4.6.1 Each BCP must clearly identify information deemed vital for the recovery of critical business and support functions in the event of a disaster as well as the relevant protection measures to be taken for protecting vital information. Licensees must refer to Chapter GR-1 when identifying vital information for business continuity. Vital information includes information stored on both electronic and non-electronic media.

OM-4.6.2 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-4.7 Other Policies Standards, and Processes

Employee Awareness and Training Plan

OM-4.7.1 **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-4.7.2 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-4.7.3 **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, 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 as well as the public in general.**

OM-4.7.4 **The BCP must clearly indicate who may speak to the media and other key external parties, and have pre-arrangements for redirecting external communications to designated staff during a disaster. Important contact numbers and e-mail addresses of key external parties must be kept in a readily accessible manner (e.g. in wallet cards or licensees' intranet).**

OM-4.7.5 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-4.7 Other Policies, Standards and Processes (continued)

OM-4.7.6 As regards internal communication, the BCP should set out how the status of recovery can be promptly and consistently communicated to all staff, 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).

Disclosure Requirements

OM-4.7.7 **Licensees must disclose how their BCP addresses the possibility of a future significant business disruption and how the licensee will respond to events of varying scope. Licensees must also state whether they plan to continue business during disruptions and the planned recovery time. The licensees might make these disclosures on their website, or through mailing to key external parties upon request. In all cases, BCP disclosures must be reviewed and updated to address changes to the BCP.**

OM-4.8 Maintenance, Testing and Review

Testing & Rehearsal

OM-4.8.1 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-4.8.2 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 depending on the situation. The following points must be included in the annual testing:

(a) Staff evacuation and communication arrangements (e.g. call-out trees) must be validated;
(b) The alternate sites for business and technology recovery must be activated;
(c) Important recovery services provided by vendors or counterparties must form part of the testing scope;
(d) Licensees must consider testing the linkage of their back up IT systems with the primary and back up systems of service providers;
(e) If back up facilities are shared with other parties (e.g. subsidiaries of the licensee), the licensee needs to verify whether all parties can be accommodated concurrently; and
(f) Recovery of vital records must be performed as part of the testing.

OM-4.8.3 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.

OM-4.8 Maintenance, Testing and Review (continued)

Periodic Maintenance and Updating of a BCP

OM-4.8.4 Licensees must have formal procedures to keep their BCP updated with respect to any changes to their business. In the event of a plan having been activated, a review process must be carried out once normal operations are restored to identify areas for improvement. If vendors are needed to provide vital recovery services, there must be formal processes for regular (say, annual) reviews of the appropriateness of the relevant service level agreement.

OM-4.8.5 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-4.8.6 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-4.8.7 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-4.8.8 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.

OM-4.8 Maintenance, Testing and Review (continued)

Audit and Independent Review

OM-4.8.9 The internal audit function of a licensee or its external auditor 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:

(a) The adequacy of business process identification;
(b) Threat scenario development;
(c) Business impact analysis and risk assessments;
(d) The written plan;
(e) Testing scenarios and schedules; and
(f) Communication of test results and recommendations to the Board.

OM-4.8.10 Significant findings 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.

MODULE	OM:	Operational Risk Management
CHAPTER	OM-4:	Business Continuity Planning

OM-4.9 Cyber Security Risk Management

OM-4.9.1 To prepare for the eventuality of cyber-attacks, licensees must have a cyber-attack response mechanism in place. The BCP of the licensee must also be properly enhanced to account for all CBB requirements and must be regularly tested to assure that the licensee is capable of dealing with cyber-attacks.

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

OM-5.1 Physical Security Measures

External Measures

OM-5.1.1 **Public entrances to head offices and branches must be protected by measures such as steel rolling shutters, or the external doors must be of solid steel or a similar solid material of equivalent strength and resistance to fire.**

OM-5.1.2 **Other external entrances must have steel doors or be protected by steel rolling shutters. Preferably, all other external entrances should have the following security measures:**

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

OM-5.1.3 **If additional security measures to those mentioned in Paragraph OM-5.1.2 such as security cameras, motion detectors or intruder alarms are installed, the requirement for steel external doors or protection by steel rolling shutters is waived.**

OM-5.1.4 **External windows must have security measures such as anti-blast films and movement detectors. For ground floor windows, licensees may also wish to add steel grills fastened into the wall.**

OM-5.1.5 Alarm systems should have the following features:

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

Internal Measures

OM-5.1.6 **All areas where cash is handled must be screened off from customers and other staff areas.**

OM-5.1 Physical Security Measures (continued)

OM-5.1.7 **Access to areas where cash is handled must be restricted to authorised staff only. The design of the teller area should not allow customers to pass through it.**

OM-5.1.8 Panic alarm systems for staff handling cash may be installed. The choice between silent or audible panic alarms is left to individual licensees. Kick bars and/or hold up buttons may be spread throughout the teller and customer service areas and the branch manager's office.

Cash Safety

OM-5.1.9 **Cash and bearer instruments must be kept in fireproof cabinets/safes. Preferably, these cabinets/safes should be located in strong rooms.**

OM-5.1.10 **Strong rooms must be made of reinforced solid concrete, or reinforced block work. Doors to strong rooms must be steel and preferably also have a steel shutter fitted. Dual locking devices must be installed in strong room doors. Strong room doors must be located out of the sight of customers.**

OM-5.1.11 **Strong rooms must not contain any other openings except the entry door and where necessary, an air conditioning outlet. The air conditioning outlet must be protected with a steel grill.**

OM-5.1.12 **Licensees must maintain a list of all maintenance, replenishment and inspection visits by staff or other authorised parties.**

CCTV Network Systems

OM-5.1.13 **All head offices and branches must have a CCTV network which is connected to a central monitoring unit located in the head office.**

OM-5.1.14 **The location and type of CCTV cameras is left to the discretion of the licensee. 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); and
(d) The service's hall.

OM-5.1 Physical Security Measures (continued)

OM-5.1.15 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) should 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.

Training and Other Measures

OM-5.1.16 Licensees must establish the formal position of security manager. This person will be responsible for ensuring all licensee staff are given annual, comprehensive security training. Licensees must produce a security manual or procedures for staff, especially those dealing directly with customers. For licensees with three or more branches, this position must be a formally identified position. For licensees with one or two branches, the responsibilities of this position may be added to the duties of a member of management.

OM-5.1.17 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-5.1.18 Licensees 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 licensees are required to hold an insurance blanket bond (which includes theft of cash in its cover).

General Requirement

OM-5.1.19 Licensees must maintain up to date Payment Card Industry Data Security Standards (PCI-DSS) certification. The initial certification must be obtained by 31st December 2017. Failure to comply with this requirement will trigger a supervisory response, which may include formal enforcement measures, as set out in Module EN (Enforcement).

OM-5.1 Physical Security Measures (continued)

OM-5.1.19.A In order to maintain up to date PCI-DSS certification, licensees 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.

Geolocation Limitations

OM-5.1.20 **All financing companies issuing 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 card 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). This requirement must be complied with by 28th February 2018.**

Europay, MasterCard and Visa (EMV) Compliance

OM-5.1.20AA All cards (credit, charge, prepaid, etc.) issued by licensees in the Kingdom of Bahrain must be EMV compliant. Moreover, all POS must be EMV compliant for accepting cards issued in the Kingdom of Bahrain. In this context, EMV compliant means using chip and online PIN authentication. However, contactless card payment transactions, where no PIN verification is required, are permitted for small amounts i.e. up to BD 20 per transaction, provided that licensees bear full responsibility in case of fraud occurrence.

Provision of Cash Withdrawal and Payment Services through Various Channels

OM-5.1.20BB Licensees are allowed to provide payment services using various channels, including but not limited to, contactless, cardless, QR code, e-wallets, biometrics (iris recognition, facial recognition, fingerprint, voiceprint, etc.), subject to enrolling customers through registration process wherein customers' acceptance of products/services terms and conditions are documented and customers are properly authenticated.

OM-5.1 Physical Security Measures (continued)

Prohibition of Double Swiping

OM-5.1.20A **All card acquirer licensees must communicate to the concerned merchants that the CBB has directed to stop the practice of double swiping of payment cards by merchants at the merchant's POS terminals/ECR, with effect from 15th June, 2017.**

OM-5.1.20B For the purpose of Paragraph OM-5.1.20A, 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-5.1.20C For the purpose of Paragraph OM-5.1.20A, 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.

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

OM-5.1 Physical Security Measures (continued)

OM-5.1.20D All card acquirer licensees must include the following clause into the merchant agreements entered into with all their merchants and bring into force the said clause on or before 15th June, 2017: ***"Pursuant to the CBB directions and instructions, the merchant shall stop double swiping of a payment card at a merchant's point-of-sale (POS) terminal/electronic cash register (ECR) to capture or store cardholder and sensitive authentication data encoded on the magnetic stripe of a customer's payment card, after the merchant received the required card payment authorisation response. The merchant asserts its full compliance with the obligation contained in this clause and understands that any breach of this clause will expose the merchant to mandatory contractual and/or legal disciplinary actions by the relevant regulator and/or concerned Ministry."***

OM-5.1.20E All card acquirer licensees must:

(i) Educate the concerned merchants on the regulatory requirement and continue to follow up the progress of the implementation to comply within the period stipulated in Paragraph OM-5.1.20A; 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.

OM-5.1.21 Licensees must ensure, with effect from 1st October 2019, that any new POS terminals or devices support contactless payment using Near Filed Communication "NFC" technology.

OM-5.1.22 Licensees must ensure, that any payment card issued or reissued (credit, debit, prepaid and charge cards) on or after 12th October 2019 supports contactless payment using Near Field Communications "NFC" technology.

OM-5.2 Internet Security

OM-5.2.1 Licensees providing internet financial services must regularly test their systems against security breaches and verify the robustness of the security controls in place. These tests must be conducted by security professionals, such as ethical hackers, that provide penetration testing services and a vulnerability assessment of the system.

OM-5.2.2 The penetration testing referred to in Paragraph OM-5.2.1, must be conducted each year in June and December.

OM-5.2.3 The vulnerability assessment report, along with the steps taken to mitigate the risks must be maintained by the licensee for a 5-year period from the date of testing and must be provided to the CBB within two months following the end of the month where the testing took place, i.e. for the June test, the report must be submitted at the latest by 31st August and for the December test, by 28th February (see Section BR-1.6).

OM-5.3 Cyber Security Measures

OM-5.3.1 Clear ownership and management accountability of the risks associated with cyber-attacks and related risk management must be established, which cover not only the IT function but also all relevant business lines. Cyber security must be made part of the licensees IT security policy.

OM-5.3.2 The Board and senior management must ensure that the cyber security controls are periodically evaluated for adequacy, taking into account emerging cyber threats and establishing a credible benchmark of cyber security controls endorsed by the Board and senior management. Should material gaps be identified, the Board and senior management must ensure that corrective action is taken immediately.

OM-5.3.3 Licensees must report to the CBB within one week, any instances of cyber-attacks, whether internal or external, that compromise customer information or disrupt critical services that affect their operations. When reporting such instances, the licensee must provide the root cause analysis of the cyber-attack and measures taken by them to ensure that similar events do not recur.