OPERATIONAL RISK MANAGEMENT MODULE

MODULE	OM Operational Risk Management
	Table of Contents

Table of Contents (continued)

OM-5.5 Cyber Security Risk Management

Role of the Board

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

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

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

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

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

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

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

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

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

Role of Senior Management

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

(a) Create the overall cyber security risk management framework and adequately oversee its implementation;
(b) Formulate a bank-wide cyber security strategy and cyber security policy;
(c) Implement and consistently maintain an integrated, bank-wide, cyber security risk management framework, and ensure sufficient resource allocation;
(d) Monitor the effectiveness of the implementation of cyber security risk management practices and coordinate cyber security activities with internal and external risk management entities;
(e) Provide quarterly or more frequent reports to the Board on the current situation with respect to cyber threats and cyber security risk treatment;

OM-5.5 Cyber Security Risk Management (continued)

(f) Prepare quarterly or more frequent reports on all cyber incidents (internal and external) and their implications on the licensee; and

(g) Ensure that processes for identifying the cyber security risk levels across the organisation are in place and annually evaluated.

OM-5.5.11 **The senior management must ensure that:**

(a) The licensee has identified clear internal ownership and classification for all information assets and data;

(b) The licensee has maintained an inventory of the information assets and data which is reviewed and updated regularly;

(c) The cyber security staff are adequate to manage the licensee's cyber security risks and facilitate the performance and continuous improvement of all relevant cyber security controls;

(d) It provides and requires cyber security staff to attend regular cyber security update and training sessions (for example Security+, CEH, CISSP, CISA, CISM) to stay abreast of changing cyber security threats and countermeasures.

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

Cyber Security Strategy

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

Cyber Security Policy

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

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

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

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

Approach, Tools and Methodology

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

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

Prevention Controls

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

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

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

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

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

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

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

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

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

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

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

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

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

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

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

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

Cyber Risk Identification and Assessments

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

(a) Cyber threat entities including cyber criminals, cyber activists, insider threats;
(b) Methodologies and attack vectors across various technologies including cloud, email, websites, third parties, physical access, or others as relevant;
(c) Changes in the frequency, variety, and severity of cyber threats relevant to the region;
(d) Dark web surveillance to identify any plot for cyber attacks;
(e) Examples of cyber threats from past cyber attacks on the licensee if available; and
(f) Examples of cyber threats from recent cyber attacks on other organisations.

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

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

OM-5.5.24A Conventional bank licensees must subscribe to an External Attack Surface Management (EASM) platform which has the ability to continuously monitor the licensee's cyber risk exposure across its entire digital presence. The platform must include the following features at a minimum:

(a) Passive, non-intrusive methods of asset discovery to identify and inventorise digital assets;
(b) Identification of exposures, misconfigurations, potential vulnerabilities and other issues with timely data refresh/update within 24 to 48 hours, and provision of remediation guidance;
(c) Provision of security rating reflecting the effectiveness of the licensee's publicly visible controls; and
(d) Third-party risk monitoring capabilities involving routine security profiling for all vendors, suppliers, and business partners to detect potential risk spillovers.

OM-5.5 Cyber Security Risk Management (continued)

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

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

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

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

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

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

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

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

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

Cyber Incident Detection and Management

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

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

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

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

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

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

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

OM-5.5.41 Licensees should record and document in an orderly manner the incidents that have been handled and the actions that were taken by the relevant functions. In particular, the licensee should maintain an "incident log" in which all the notifications, decisions and actions taken, in relation to cyber incidents, are documented, as close as possible to the time of their occurrence. It should also include the status of the issue whether it is open or has been resolved and person in charge of resolving the issue/incident. The logs should be stored and preserved in a secure and legally admissible manner.

OM-5.5 Cyber Security Risk Management (continued)

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

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

The cyber incident severity may be classified as:

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

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

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

1. Metrics to measure impact of a cyber incident:
   (a) Duration of unavailability of critical functions and services;
   (b) Number of stolen records or affected accounts;
   (c) Volume of customers impacted;
   (d) Amount of lost revenue due to business downtime, including both existing and future business opportunities;
   (e) Percentage of service level agreements breached.

OM-5.5 Cyber Security Risk Management (continued)

2. Performance metrics for incident management:
   (a) Volume of incidents detected and responded via automation;
   (b) Dwell time (i.e. the duration a threat actor has undetected access until completely removed);
   (c) Recovery Point objectives (RPO) and recovery time objectives (RTO) satisfied.

Recovery

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

OM-5.5.46 Critical incidents are defined as incidents that trigger the BCP and the crisis management plan. Critical systems and services are those whose failure can have material impact on any of the following elements:
a) Financial situation;
b) Reputation;
c) Regulatory, legal and contractual obligations; and
d) Operational aspects and delivery of key products and services.

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

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

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

OM-5.5 Cyber Security Risk Management (continued)

OM-5.5.50 Conventional bank licensees must define a program for exercising the various response mechanisms, taking into account the various types of exercises such as attack simulations, "war games" and "table top" exercises, and with reference to the relevant stakeholders such as technical staff, crisis management team, decision-makers and spokespersons.

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

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

Cyber Security Insurance

OM-5.5.53 Conventional bank licensees must arrange to seek cyber risk insurance cover from a suitable insurer, following a risk-based assessment of cyber security risk is undertaken by the respective licensee and independently verified by the insurance company. The insurance policy may include some or all of the following types of coverage, depending on the risk assessment outcomes:

(a) Crisis management expenses, such as costs of notifying affected parties, costs of forensic investigation, costs incurred to determine the existence or cause of a breach, regulatory compliance costs, costs to analyse the insured's legal response obligations;

(b) Claim expenses such as costs of defending lawsuits, judgments and settlements, and costs of responding to regulatory investigations; and

(c) Policy also provides coverage for a variety of torts, including invasion of privacy or copyright infringement. First-party coverages may include lost revenue due to interruption of data systems resulting from a cyber or denial of service attack and other costs associated with the loss of data collected by the insured.

OM-5.5 Cyber Security Risk Management (continued)

Training and Awareness

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

OM-5.5.55 The licensee must ensure that all employees receive adequate training on a regular basis, in relation to cyber security and the threats they could encounter, such as through testing employee reactions to simulated cyber attack scenarios. All relevant employees must be informed on the current cyber security breaches and threats. Additional training should be provided to 'higher risk staff'.

OM-5.5.56 The conventional bank licensees must ensure that role specific cyber security training is provided on a regular basis to relevant staff including:
(a) Executive board and senior management;
(b) Cyber security roles;
(c) IT staff; and
(d) Any high-risk staff as determined by the licensee.

Reporting to CBB

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

OM-5.5 Cyber Security Risk Management (continued)

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

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

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

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

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