RISK MANAGEMENT MODULE

MODULE	RM (Risk Management)

Table of Contents

RM-9.1 Cyber Security Risk Management

RM-9.1.1 **This Chapter is applicable to Category 1 investment firm licensees and Category 2 investment firm licensees. Category 3 investment firm licensees providing digital financial advice must also apply the requirements in this Chapter.**

Role of the Board

RM-9.1.2 **The Board of investment firm licensees must ensure that the licensee has a robust cyber security risk management framework to comprehensively manage the licensee's cyber security risk and vulnerabilities. The Board must approve the cyber security policy and establish clear ownership, decision-making and management accountability for risks associated with cyber-attacks and related risk management and recovery processes. The Board must also 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.

RM-9.1.3 **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 A – Cyber security Control Guidelines. At the broader level, the Cyber security framework should be consistent with the licensee's risk management framework.**

RM-9.1.4 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.

RM-9.1.5 **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. Cyber security must be an item for discussion at Board or Board sub-committee meetings.**

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.6 **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. Overseas investment firm 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.**

RM-9.1.7 The Board should ensure that appropriate resources are allocated to the cyber security risk management function for implementing the cyber security framework.

RM-9.1.8 **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.**

RM-9.1.9 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.

RM-9.1 Cyber Security Risk Management (continued)

Role of Senior Management

RM-9.1.10 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 an organisation-wide cyber security strategy and cyber security policy;
(c) Implement and consistently maintain an integrated, organisation-wide, cyber security risk management framework, and ensure sufficient resource allocation;
(d) Monitor the effectiveness of the implementation of cyber security risk management practices and coordinate cyber security activities with internal and external risk management entities;
(e) Provide quarterly or more frequent reports to the Board on the current situation with respect to cyber threats and cyber security risk treatment;
(f) Prepare quarterly or more frequent reports on all cyber incidents (internal and external) and their implications on the licensee; and
(g) Ensure that processes for identifying the cyber security risk levels across the licensee are in place and annually evaluated.

RM-9.1.11 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.

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.12 With respect to Subparagraph RM-9.1.11(a), data classification entails analyzing the data the licensee retains, determining its importance and value, and then assigning it to a category. When classifying data, the following aspects of the policy should be determined:

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

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

Cyber Security Strategy

RM-9.1.13 **An organisation-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.

RM-9.1.14 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 A provides cyber security control guidelines that can be used as reference to support the licensee's cyber security strategy and cyber security policy.

RM-9.1 Cyber Security Risk Management (continued)

Cyber Security Policy

RM-9.1.15 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.

RM-9.1 Cyber Security Risk Management (continued)

Approach, Tools and Methodology

RM-9.1.16 **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.**

RM-9.1.17 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 licensee'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 licensee. 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

RM-9.1.18 **A 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 ;

(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);

RM-9.1 Cyber Security Risk Management (continued)

(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 licensee 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.

RM-9.1.19 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".

RM-9.1.20 Licensees should subscribe to one of the Cyber Threat Intelligence services in order to stay abreast of emerging cyber threats, cybercrime actors and state of the art tools and security measures.

RM-9.1.21 Licensees must use a single unified email domain for communication with customers to prevent abuse by third parties. For example, ensuring that all emails are sent from xyz@licensee.com and not utilizing shortened services or third party email providers. Licensees must not use URLs in SMS or other short messages.

RM-9.1 Cyber Security Risk Management (continued)

Cyber Risk Identification and Assessments

RM-9.1.22 **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.

RM-9.1.23 **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.**

RM-9.1.24 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.

RM-9.1.25 **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.**

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.26 With respect to Paragraph RM-9.1.25, 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.

RM-9.1.27 **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.**

RM-9.1.28 **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.

RM-9.1.29 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.

RM-9.1.30 **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.**

RM-9.1 Cyber Security Risk Management (continued)

Cyber Incident Detection and Management

RM-9.1.31 **Licensees must implement cyber security incident management processes to ensure timely detection, response and recovery for cyber security incidents. This includes implementing a monitoring system for log correlation and anomaly detection.**

RM-9.1.32 Licensees 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.

RM-9.1.33 Licensees should retain the logs and other information from the monitoring system for detecting cyber incidents, including "low-and-slow" attacks, in order to facilitate incident investigations, for 5 years or longer.

RM-9.1.34 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.

RM-9.1.35 **Licensees must define roles and responsibilities and assign adequate resources to detect, identify, investigate and respond to cyber incidents that could impact the licensee's infrastructure, services and customers. Such responsibilities must include log correlation, anomaly detection and maintaining the licensee's asset inventory and network diagrams.**

RM-9.1.36 **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 monitoring system must be updated with new use cases and rule sets which are capable of detecting the current cyber incident scenarios.**

RM-9.1.37 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.

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.38 **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 RM-9.1.57 for the requirement to report to CBB.**

RM-9.1.39 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 licensee'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.

RM-9.1.40 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.

RM-9.1.41 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.

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.42 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); and
(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.

RM-9.1.43 Licensees should determine the effects of the cyber incident on customers and to the wider financial 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.

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.44 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; and
   (e) Percentage of service level agreements breached.
2. Performance metrics for incident management:
   (a) Volume of incidents detected and responded via automation;
   (b) Dwell time (i.e. the duration a threat actor has undetected access until completely removed); and
   (c) Recovery Point objectives (RPO) and recovery time objectives (RTO) satisfied.

Recovery

RM-9.1.45 **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.**

RM-9.1.46 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.

RM-9.1.47 **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.**

RM-9.1.48 **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.**

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.49 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.

RM-9.1.50 **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.**

RM-9.1.51 **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.**

RM-9.1.52 **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

RM-9.1.53 **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.

RM-9.1 Cyber Security Risk Management (continued)

Training and Awareness

RM-9.1.54 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.

RM-9.1.55 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'.

RM-9.1.56 The 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

RM-9.1.57 Licensees must submit Section A of the Cyber Security Incident Report (Appendix RM-1) to CBB's cyber incident reporting email, incident.report@cbb.gov.bh, immediately (within one hour) upon occurrence or detection of any cyber incidents, whether internal or external, that compromises customer information or disrupts critical services that affect operations. Licensees may contact the CBB for any queries/consultation by phone on 39965693/66332133.

RM-9.1.58 Following the submission referred to in Paragraph RM-9.1.57, the licensee must submit to CBB Section B of the Cyber Security Incident Report (Appendix RM-1) within 5 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.

RM-9.1 Cyber Security Risk Management (continued)

RM-9.1.59 With regards to the submission requirement mentioned in Paragraph RM-9.1.58, the licensee should submit the report with as much information as possible even if all the details have not been obtained yet.

RM-9.1.60 **The penetration testing report as per Paragraph RM-9.1.28, 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 (see Section BR-4A.2).**

Appendix A – Cyber Security Control Guidelines

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

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

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

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

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

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

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

IDENTIFY

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

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

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

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

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

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

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

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

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

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

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

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

PROTECT

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

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

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

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

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

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

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

1. A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
2. A System Development Life Cycle to manage systems is implemented
3. Configuration change control processes are in place.
4. Backups of information are conducted, maintained, and tested.
5. Policy and regulations regarding the physical operating environment for licensee's assets are met.

6. Data is destroyed according to policy.
7. Protection processes are improved.
8. Effectiveness of protection technologies is shared.
9. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
10. Response and recovery plans are tested.
11. Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening).
12. A vulnerability management plan is developed and implemented.

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

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

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

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

DETECT

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

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

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

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

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

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

RESPOND

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

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

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

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

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

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

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

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

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

RECOVER

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

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

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

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

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