CRYPTO-ASSET MODULE

Table of Contents

MODULE	CRA (Crypto-asset)
	Table of Contents (continued)

CRA-5.8 Cyber Security

General Requirements

CRA-5.8.1 **A licensee must establish and maintain an effective cyber security program to ensure the availability and functionality of the licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering. The cyber security program must be designed to perform, at the minimum, the following five core cyber security functions:**

(a) identify internal and external cyber security risks by, at a minimum, identifying the information stored on the licensee's systems, the sensitivity of such information, and how and by whom such information may be accessed;

(b) protect the licensee's electronic systems, and the information stored on those systems, from unauthorized access, use, or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures;

(c) detect system intrusions, data breaches, unauthorized access to systems or information, malware, and other cyber security events;

(d) respond to detected cyber security events to mitigate any negative effects; and

(e) recover from cyber security events and restore normal operations and services.

CRA-5.8.1A **Licensees must have a robust cyber security risk management framework that 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.

CRA-5.8.1B **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. Broadly, the cyber security risk management framework should be consistent with the licensee's risk management framework.**

CRA-5.8.1C Senior management, and where appropriate, the boards, should receive comprehensive reports, 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;

CRA-5.8 Cyber Security (continued)

(d) Updates on latest internal or relevant external cyber security incidents; and
(e) Results from penetration testing exercises.

CRA-5.8.1D Licensees may establish a cyber security committee that is headed by an independent senior manager from a control function (like 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.

Roles and Responsibilities of the Board

CRA-5.8.2 **The board must provide oversight and accord sufficient priority and resources to manage cyber security risk, as part of the licensee's overall risk management framework.**

CRA-5.8.3 **In discharging its oversight functions, the board must:**

(a) Ensure that the licensee's strategy, policy and risk management approach relating to cyber security are presented for the board's deliberation and approval;

(b) Ensure that the approved cyber security risk policies and procedures are implemented by the management;

(c) Monitor the effectiveness of the implementation of the licensee's cyber security risk policies and procedures and ensure that such policies and procedures are periodically reviewed, improved and updated, where required. This may include setting performance metrics or indicators, as appropriate, to assess the effectiveness of the implementation of cyber security risk policies and procedures;

(d) Ensure that adequate resources are allocated to manage cyber security including appointing a qualified person as Chief Information Security Officer ("CISO") with appropriate authority to implement the cyber security strategy. The CISO is the person responsible and accountable for the effective management of cyber security;

(e) [This Subparagraph was deleted in April 2023];

(f) Ensure that the impact of cyber security risk is adequately assessed when undertaking new activities, including but not limited to any new products, investment decision, merger and acquisition, adoption of new technology and outsourcing arrangements; and

CRA-5.8 Cyber Security (continued)

(g) Ensure that adequate resources are allocated to manage cyber security including appointing a qualified person as Chief Information Security Officer ("CISO"). The CISO is the person responsible and accountable for the effective management of cyber security;

(h) Ensure that the management continues to promote awareness on cyber resilience at all levels within the entity;

(i) Ensure that the impact of cyber security risk is adequately assessed when undertaking new activities, including but not limited to any new products, investments decision, merger and acquisition, adoption of new technology and outsourcing arrangements; and

(j) Ensure that the board keeps itself updated and is aware of new or emerging trends of cyber security threats and understand the potential impact of such threats to the licensee.

Roles and Responsibilities of the Management

CRA-5.8.4

The management is responsible for:

(a) Establishing and implementing cyber security policies and procedures that commensurate with the level of cyber security risk exposure and its impact on the licensee. These policies and procedures must take into account the following:

(i) The sensitivity and confidentiality of data which the licensee maintains;

(ii) Vulnerabilities of the licensee's information systems and operating environment across the licensee; and

(iii) The existing and emerging cyber security threats.

(b) Ensuring that employees, agents (where relevant) and third party service providers are aware and understand the cyber security risk policies and procedures, the possible impact of various cyber security threats and their respective roles in managing such threats;

(c) Recommending to the board on appropriate strategies and measures to manage cyber security risk, including making necessary changes to existing policies and procedures, as appropriate; and

(d) Reporting to the board of any cyber security breaches and periodically update the board on emerging cyber security threats and their potential impact on the entity.

CRA-5.8 Cyber Security (continued)

CRA-5.8.4A **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) Employees responsible for cyber security are adequate to manage the licensee's cyber security risks and facilitate the performance and continuous improvement of all relevant cyber security controls; and

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

CRA-5.8.4B With respect to Paragraph CRA-5.8.4A(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 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. The owner of data (i.e. the relevant business function) should be involved in such classification.

Cyber Security Strategy

CRA-5.8.4C **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.

CRA-5.8 Cyber Security (continued)

CRA-5.8.4D 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 a reference to support the licensee's cyber security strategy and cyber security policy.

Cyber Security Risk Policy

CRA-5.8.5 **Licensees must implement a written cyber security risk policy setting out the licensee's Board approved policies and related procedures that are approved by senior management, for the protection of its electronic systems and client data stored on those systems. This policy must be reviewed and approved by the licensee's board of directors at least annually. The cyber security policy, among others, must address the following areas:**

(a) 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, recovery time objectives and occurrence/severity of cyber security breaches. The statement must also consider the impact on clients, potential negative media publicity, potential regulatory penalties, financial loss etc.;

(b) Strategy and measures to manage cyber security risk encompassing prevention, detection and recovery from a cyber security breach;

(c) Roles, responsibilities and lines of accountabilities of the board, the board committees, person responsible and accountable for effective management of cyber security risk and key personnel involved in functions relating to the management of cyber security risk (such as information technology and security, business units and operations, risk management, business continuity management and internal audit);

(d) Processes and procedures for the identification, detection, assessment, prioritisation, containment, response to, and escalation of cyber security breaches for decision-making;

CRA-5.8 Cyber Security (continued)

(e) Processes and procedures for the management of outsourcing, system development and maintenance arrangements with third-party service providers, including requirements for such third-party service providers to comply with the licensee's cyber security risk policy;

(f) Communication procedures that will be activated by the licensee in the event of a cyber security breach, which include reporting procedures, information to be reported, communication channels, list of internal and external stakeholders and communication timeline; and

(g) Other key elements of the information security and cyber security risk management including the following:
   (i) information security;
   (ii) data governance and classification;
   (iii) access controls;
   (iv) business continuity and disaster recovery planning and resources;
   (v) capacity and performance planning;
   (vi) systems operations and availability concerns;
   (vii) systems and network security;
   (viii) systems and application development and quality assurance;
   (ix) physical security and environmental controls;
   (x) client data privacy;
   (xi) vendor and third-party service provider management;
   (xii) monitoring and implementing changes to core protocols not directly controlled by the licensee, as applicable;
   (xiii) incident response; and
   (xiv) System audit.

CRA-5.8.6 [This Paragraph was deleted in April 2023].

CRA-5.8.7 [This Paragraph was deleted in April 2023].

CRA-5.8 Cyber Security (continued)

Prevention

CRA-5.8.8 A licensee must conduct regular assessments as part of the licensee's compliance programme to identify potential vulnerabilities and cyber security threats in its operating environment which could undermine the security, confidentiality, availability and integrity of the information assets, systems and networks.

CRA-5.8.9 The assessment of the vulnerabilities of the licensee's operating environment must be comprehensive, including making an assessment of potential vulnerabilities relating to the personnel, parties with whom a licensee deals with, systems and technologies adopted, business processes and outsourcing arrangements.

CRA-5.8.10 A licensee must develop and implement preventive measures to minimise the licensee's exposure to cyber security risk.

CRA-5.8.11 Preventive measures referred to in Paragraph CRA-5.8.10 above must include, at a minimum, the following:

(a) Deployment of End Point Protection (EPP) and End Point Detection and Response (EDR) including anti-virus software and malware programs to detect, prevent and isolate malicious code;
(b) Layering systems and systems components;
(c) Use of firewalls for network segmentation including use of Web Application Firewalls (WAF), where relevant, 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 testing at software development stage as well as after deployment to limit the number of vulnerabilities;
(e) Penetration testing of existing systems and networks;
(f) Use of authority matrix to limit privileged internal or external access rights to systems and data;
(g) 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);

CRA-5.8 Cyber Security (continued)

(h) Use of a Secure Web Gateway to limit browser based cyber-attacks, malicious websites and enforce organization policies;

(i) 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; and

(j) 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.

CRA-5.8.11A Licensees should also implement the following prevention controls in the following areas:

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

(b) Controls 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 (e.g. Network access control); and

(c) Identity and access management controls to limit the exploitation and monitor the use of privileged and non-privileged accounts.

CRA-5.8.11B **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:**

(a) SPF "Sender Policy Framework";

(b) DKIM "Domain Keys Identified Mail"; and

(c) DMARC "Domain-based Message Authentication, Reporting and Conformance".

CRA-5.8.11C **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.**

CRA-5.8.11D **Licensees must use a single unified private email domain or its subdomains for communication with clients to prevent abuse by third parties. Licensees must not utilise third-party email provider domains for communication with clients. The email domains must comply with the requirements of Paragraph OM-5.8.11B with respect to SPF, DKIM and DMARC.**

CRA-5.8 Cyber Security (continued)

CRA-5.8.11E For the purpose of Paragraph CRA-5.8.11D, licensees with subsidiaries or branches outside Bahrain will be allowed to use additional domains subject to CBB's review. Licensees may be allowed, subject to CBB's review, for their clients to receive emails from third-party service providers for specific services offered by such third-parties provided the clients were informed and agreed on such an arrangement. Examples of such third-party services include informational subscription services and document management services.

CRA-5.8.11F **Licensees must comply with the following requirements with respect to URLs or other clickable links in communications with clients:**

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

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

(c) Implement measures to allow clients to verify the legitimacy of the links which may include:

(i) clear instructions on the licensee's website/app where the link is sent as a result of client action on the licensee's website/app;

(ii) communication with client such as a phone call informing the client 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 client with the link;

(iv) use of other verification measures like OTP, password or biometric authentication; and

(d) Create client awareness campaigns to educate their clients on the risk of fraud related to links they receive in SMS, short messages and emails with clear instructions to clients 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 client request or action. Licensees may also train their clients by sending fake phishing messages.

CRA-5.8.12 **[This Paragraph was deleted in April 2023].**

CRA-5.8 Cyber Security (continued)

CRA-5.8.13 [This Paragraph was deleted in April 2023].

Cyber Risk Identification and Assessments

CRA-5.8.13A **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 where applicable; and

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

CRA-5.8.13B **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.**

CRA-5.8.13C 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-5.5.13CC **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.

CRA-5.8 Cyber Security (continued)

CRA-5.8.13D **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 should be conducted for internal technology and weekly or more frequent assessments for external public facing services and systems.**

CRA-5.8.13E With respect to Paragraph CRA-5.8.13D, 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.

CRA-5.8.13F **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.**

CRA-5.8.13G **All licensees must perform vulnerability assessment and 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 internally at periodic intervals by employees having adequate expertise and competency in such testing;
(e) Be performed, twice a year, by external independent third parties who are rotated out at least every two years; and
(f) Be performed on either the production environment or on non-production exact replicas of the production environment.

CRA-5.8.13H The CBB may require additional third-party security reviews to be performed as needed.

CRA-5.8 Cyber Security (continued)

CRA-5.8.13I **The time period between two consecutive penetration test and the vulnerability assessment by an independent third party, referred to in Paragraph CRA-5.8.13G(e) must be 6 months and the report on such testing must be provided to CBB within two months following the end of the month where the testing took place. The vulnerability assessment and penetration testing reports must include the vulnerabilities identified and a full list of 'passed' tests and 'failed' tests together with the steps taken to mitigate the risks identified.**

Cyber Incident Detection and Management

CRA-5.8.14 **[This Paragraph was deleted in April 2023].**

CRA-5.8.14A **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.**

CRA-5.8.14B 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.

CRA-5.8.14C 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 12 months or longer.

CRA-5.8.14D 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.

CRA-5.8.14E **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 clients. Such responsibilities must include log correlation, anomaly detection and maintaining the licensee's asset inventory and network diagrams.**

CRA-5.8 Cyber Security (continued)

CRA-5.8.14F **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.**

CRA-5.8.14G 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.

CRA-5.8.14H **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 CRA-5.8.33 for the requirement to report to the CBB.**

CRA-5.8.14I 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:

(a) **Incident Owner:** An individual who 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.

(b) **Spokesperson:** An individual, who 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.

(c) **Record Keeper:** An individual who 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 should serve as an accurate source of reference for after-action reviews to improve future cyber incident detection and response activities.

CRA-5.8 Cyber Security (continued)

CRA-5.8.14J 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.

CRA-5.8.14K 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 the person in charge of resolving the issue/incident. The logs should be stored and preserved in a secure and legally admissible manner.

CRA-5.8.14L 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 is 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 clients, data leakage, unavailability of data, data destruction/corruption, reputational damage).
(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 caused 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.

CRA-5.8.14M Licensees should determine the effects of the cyber incident on clients and to the wider financial system as a whole and report the results of such an assessment to the CBB if it is determined that the cyber incident may have a systemic impact.

CRA-5.8 Cyber Security (continued)

CRA-5.8.14N Licensees should establish metrics to measure the impact of a cyber incident and to report to management the performance of response activities. Examples include:

(a) Metrics to measure impact of a cyber incident:
   (i) Duration of unavailability of critical functions and services;
   (ii) Number of stolen records or affected accounts;
   (iii) Volume of clients impacted;
   (iv) Amount of lost revenue due to business downtime, including both existing and future business opportunities; and
   (v) Percentage of service level agreements breached.

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

CRA-5.8.15 **[This Paragraph was deleted in April 2023].**

CRA-5.8.16 **[This Paragraph was deleted in April 2023].**

CRA-5.8.17 **[This Paragraph was deleted in April 2023].**

CRA-5.8.18 **[This Paragraph was deleted in April 2023].**

CRA-5.8.19 **[This Paragraph was deleted in April 2023].**

CRA-5.8.19A **[This Paragraph was deleted in April 2023].**

CRA-5.8.20 **[This Paragraph was deleted in April 2023].**

CRA-5.8.20A **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 levels of service during the downtime and determine how much time the licensee will require to return to full service and operations.**

CRA-5.8 Cyber Security (continued)

CRA-5.8.20B 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;
(d) Operational aspects; and
(e) Delivery of key products and services.

CRA-5.8.20C **Licensees must define a program for recovery activities for the purpose of 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 within 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, clients and other relevant external stakeholders as may be necessary.**

CRA-5.8.20D **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.**

CRA-5.8.20E 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 clients.

CRA -5.8.20F **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 "tabletop" exercises, and with reference to the relevant stakeholders such as technical staff, crisis management team, decision-makers and spokespersons.**

CRA-5.8.20G **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.**

CRA-5.8 Cyber Security (continued)

CRA-5.8.21 **[This Paragraph was deleted in April 2023].**

CRA-5.8.22 **A 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 breach.**

Chief Information Security Officer

CRA-5.8.23 **A licensee's CISO, as referred to in Paragraph CRA-5.8.3(d), is responsible for overseeing and implementing the licensee's cyber security program and enforcing its cyber security policy. The CISO must report to an independent risk management function or the licensee must incorporate the responsibilities of cyber security risk into the risk management function.**

CRA-5.8.24 **[This Paragraph was deleted in January 2020].**

IT System Audit

CRA-5.8.25 **[This Paragraph was deleted in January 2020].**

CRA-5.8.25A **[This Paragraph was deleted in April 2023].**

CRA-5.8.26 **[This Paragraph was deleted in April 2023].**

CRA-5.8.27 **[This Paragraph was deleted in April 2023].**

Cyber Risk Insurance

CRA-5.8.28 **A licensee, based on the assessment of cyber security risk exposure and with an objective to mitigate cyber security risk, must evaluate and consider the option of availing cyber risk insurance. The evaluation process to determine suitability of cyber risk insurance as a risk mitigant must be undertaken on a yearly basis and be documented by the licensee.**

CRA-5.8.29 The cyber risk insurance policy, referred to in Paragraph CRA-5.8.28, 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 of analysing the licensee's legal response obligations;

CRA-5.8 Cyber Security (continued)

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

(c) Coverage for a variety of torts, including invasion of privacy or copyright infringement; and

(d) Coverages relating to loss of 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 licensee.

Training and Awareness

CRA-5.8.30 **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.**

CRA-5.8.31 **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'.**

CRA-5.8.32 **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 the CBB

CRA-5.8.33 **Upon occurrence or detection of any cyber security incident or detection of any unplanned outages, whether internal or external, that compromises client information or disrupts critical services that affect operations, licensees must contact the CBB, immediately (within one hour), on 17547477 and submit Section A of the Cyber Security Incident Report (Appendix-B) to the CBB's cyber incident reporting email, incident.cra@cbb.gov.bh, as soon as possible, but not later than two hours, following occurrence or detection of any cyber incidents.**

CRA-5.8 Cyber Security (continued)

CRA-5.8.34 **Following the submission referred to in Paragraph CRA 5.8.33, the licensee must submit to the CBB Section B of the Cyber Security Incident Report (Appendix B) 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 clients, 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.**

CRA-5.8.35 With regards to the submission requirement mentioned in Paragraph CRA-5.8.34, the licensee should submit the report with as much information as possible even if all the details have not been obtained yet.

CRA-5.8.36 **The vulnerability assessment and penetration testing report (see Paragraph CRA-5.8.13I), 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.**