澳 門 金 融 管 理 局
AUTORIDADE MONETÁRIA DE MACAU

Circular No. 016/B/2019-DSB/AMCM

Date: 18 December 2019

Guideline on Cyber Resilience

The Monetary Authority of Macao (AMCM), under the powers conferred by Article 9 of the Charter approved by Decree-Law No.14/96/M of 11th March and by Article 6 of the Financial System Act of Macao approved by Decree-Law No. 32/93/M of 5th July, establishes the following:

1. INTRODUCTION

1.1. With new cyber threats emerging every day, new cyber risks are introduced to institutions' environment. Financial sector is considered as one of the industries with high cyber risks and impact. Financial institutions across the globe have been taking proactive steps to address cyber risks. Over the years, recognizing the increasing cyber-attacks on the financial industry around the world, financial institutions have continuously placed additional effort to enhance their cyber resilience and benchmark its cybersecurity implementation with reference to industry practices and international standards with an aim to understand the cyber risk exposure and effectiveness of cybersecurity controls to protect the organization.

1.2. Given that threats of cyber-attacks are evolving, this Guideline is established for the authorized institutions[1] in order to provide a set of cybersecurity controls and measures for the Macao financial sector regarding cyber risk management and to enhance the capability in defending cyber attacks. Apart from existing regulatory requirements and guidelines[2], authorized institutions should always take into account of the latest industry standards and practices[3] to ensure a sound cyber risk management practice.

1.3. Authorized institutions are expected to conduct regular assessment in relation to the following supervisory requirements. Since the technologies adopted by the financial industry and cyber threats are evolving rapidly, it

[1] Credit institutions and the institutions mentioned herein are collectively referred to as "authorized institutions".

[2] Including but not limited to "Guideline on Risk Management of Electronic Banking" (Circular no. 003/B/2008-DSB/AMCM), "Guideline on Outsourcing" (Circular no. 032/B/2009-DSB/AMCM), "Guideline on Business Continuity Management" (Circular no. 033/B/2009-DSB/AMCM) and Incident Reporting Measures for Major Emergencies (Circular no. 012/B/2016-DSB/AMCM).

[3] Refer to Appendix B for references of industry standards and practices.

should be noted that the recommendations suggested in this Guideline should not be considered definitive. Authorized institutions should always take into account the other relevant industry standards and practices to ensure that their cyber risk management are sufficient and consistent with the nature and scale of authorized institutions' business.

1.4. This Guideline sets forth the key principles in managing the risks associated with cybersecurity. All authorized institutions are expected to adopt the key principles that will assist them in establishing a sound and robust cyber risk management process. The Guideline is applicable to the following financial institutions authorized under the provisions of the Financial System Act (FSA) approved by Decree-Law no. 32/93/M of 5th July:

(a) credit institutions either locally incorporated or being branches of overseas banks in Macao;
(b) financial intermediaries and other financial institutions.

The Guideline is also applicable to the following financial institutions authorized under the provisions of specific laws and regulations other than the FSA:

(c) finance companies authorized under Decree-Law no. 15/83/M of 26th February; and
(d) institutions authorized under Decree-Law no. 15/97/M of 5th May to carry out cash remittance activities in Macao.

1.5. The AMCM has taken into account of the risk management principles and sound practices in similar cyber resilience standards, guidelines and frameworks from other regulatory authorities and international standards[4], when developing this guideline. Domains similar to those used in such standards, guidelines and frameworks have been adopted to organize

[4] Reference of cyber resilience standards, guidelines and frameworks from other regulatory authorities and international standards, for example:

- "Guidance on cyber resilience for financial market infrastructures" (June 2016) issued by Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions (CPMI-IOSCO)
- "Cybersecurity assessment tool" (May 2017) issued by United States Federal Financial Institutions Examination Council (FFIEC)
- "Fundamental elements of cybersecurity for the financial sector" (October 2016) issued by Group of 7 (G7)
- "Framework for improving critical infrastructure cybersecurity" (April 2018) issued by United States National Institute of Standard and Technology (NIST)
- "Cyber resilience oversight expectations for financial market infrastructures" (December 2018) issued by European Central Bank

related requirements. Authorized institutions are also encouraged to read and understand the main principles of these documents.

2. RISK MANAGEMENT CHALLENGES POSED BY CYBERSECURITY

2.1. As echoed by various risk management principles and sound practices, the cyber risk should be managed as a part of the authorized institution's overall operational risk management framework. Some unique characteristics of cyber risk present challenges to authorized institutions' traditional operational risk management frameworks.

2.2. Firstly, a distinguishing characteristic of sophisticated cyber-attacks is the persistent nature of a campaign conducted by a motivated attacker. The presence of an active, persistent and sometimes sophisticated adversary in cyber-attacks means that, unlike most other sources of risk, malicious cyber-attacks are often difficult to be identified or fully eradicated and the breadth of damage is as well difficult to be determined.

2.3. Secondly, there is a broad range of entry points through which an authorized institution could be compromised. As a result of their interconnectedness, cyber-attacks could come through linked financial institutions, service providers, vendors and vendor products. Authorized institutions themselves could become a channel to further propagate cyber-attacks – for example, via the distribution of malware to interconnected entities. Unlike physical operational disruptions, cyber risks posed by an interconnected entity are not necessarily related to the degree of that entity's relevance to the authorized institution's business. From a cybersecurity perspective, the small-value or small-volume participant or a vendor providing non-critical services may be as risky as a major participant or a critical service provider[5]. Internally, the risk of insider threat arising from rogue or careless staff opens up additional channels for possible compromises.

2.4. Thirdly, certain cyber-attacks can render some risk management and business continuity arrangements ineffective. For example, automated system and data replication arrangements that are designed to help preserve sensitive data and software in the event of a physical disruptive event might in some instances fuel the propagation of malware and corrupted data to backup systems. Overall, a cyber-attack's potential to cause significant

[5] Service provider who support critical business functions.

service disruptions to the broader financial system dictates the urgency of having an effective approach in place to response to such attack, and it requires a prudent incident response mechanism to minimise the probability that service resumption will introduce additional cyber risks to the institution.

2.5. Fourthly, cyber-attacks can be stealthy and propagate rapidly within a network of systems. For example, the attacker can exploit unknown vulnerabilities and weak links in systems and protocols to cause disruptions and/or infiltrate an authorized institution's internal network. Malwares designed to take advantage of such latent vulnerabilities may circumvent controls. To minimise the impact of such attacks, authorized institution should equip with capabilities to swiftly detect, respond to, contain and recover from such attacks.

3. CYBER RISK MANAGEMENT DOMAINS

3.1. This Guideline is presented in eight domains that should be addressed across an authorized institution's cybersecurity resilience framework. They are summarized below and discussed more specially in Sections 4 to 11.

a) *Governance.* Consistent with effective management of other forms of risk faced by an authorized institution, sound governance is the key to good cyber risk management. Authorized institution should establish, implement and enhance its approach to managing cyber risks. Therefore, a clear and comprehensive cyber resilience framework should be established and guided by a cyber resilience strategy, which define the cyber resilience objective and set out people, process and technology requirements to achieve such objective. It is also important that clear roles and responsibilities of the board[6] and senior management are established, with a good culture of recognizing the importance of cybersecurity. The requirements are further elaborated in Section 4.

b) *Identification.* Without a proper understanding of the authorized institution's ecosystem, authorized institutions may risk having an

[6] In the case of branches of overseas incorporated banks, the reference to the "board of directors / the Board" in this Guideline refers to, depending on the circumstances, either the branches' local management or, the management at the head office responsible for the operations of the branches. In the case of a Macao incorporated bank, the reference to the "board of directors / the Board" in this Guideline includes any director or committee that is assigned to handle matters that require the board's review / approval but arise between full board meetings.

inadequate coverage when implementing cybersecurity controls. Authorized institutions should develop an organizational understanding to identify and classify business processes, systems, people, assets, data, and external dependencies. Understanding the business context, the resources that support critical functions, and the related cyber risks enables authorized institutions to focus and prioritize its efforts and align with its risk management strategy. The requirements are further elaborated in Section 5.

c) *Protection.* Without an effective security controls on the system and processes, the confidentiality, integrity and availability of data and system could be compromised. Authorized institutions should implement appropriate safeguards to ensure delivery of critical services and to contain the impact of a potential cybersecurity event. The requirements are further elaborated in Section 6.

d) *Detection.* Timely detection allows authorized institutions to have proper lead time to deploy countermeasure against cybersecurity event. Authorized institutions should define the appropriate activities to identify the occurrence of a cybersecurity event. The requirements are further elaborated in Section 7.

e) *Respond and recovery.* It is important for authorized institutions to contain and reduce the impact of a cybersecurity incident. Authorized institutions should maintain plans for responding to cybersecurity events as well as for resilience and recovery of any services that were impaired during a cybersecurity incident. The requirements are further elaborated in Section 8.

f) *Testing.* The elements of authorized institutions' cyber resilience framework should be rigorously tested to determine their overall effectiveness. Authorized institutions should adopt sound testing mechanisms to identify gaps against stated resilience objectives and to provide credible and meaningful inputs to authorized institutions' management of cyber risks. The requirements are further elaborated in Section 9.

g) *Situational awareness.* Strong situational awareness can significantly enhance an authorized institution's ability to understand and pre-empt cyber events, and to effectively detect, respond to and recover from cyber-attacks that are not prevented. Authorized institutions should proactively monitor the cyber threat landscape and participate in the information-sharing initiatives to further enhance authorized institutions' approach in cyber resilience. The requirements are further elaborated in Section 10.

h) *Learning and evolving.* As cyber threat is evolving quickly, it is important for authorized institutions to have an adaptive cyber resilience framework. Authorized institutions should instil a culture of cyber risk awareness and perform ongoing re-evaluation and improvement activities of the cyber resilience posture at every level within the organisation. The requirements are further elaborated in Section 11.

4. **GOVERNANCE**

4.1. Board and Senior Management

4.1.1. *Board and Senior Management Responsibilities.* The primary responsibilities for cyber risk management rests with the board and senior management of authorized institutions. The board should establish and approve the cyber risk tolerance by defining the level of cyber risk that the authorized institution is willing to assume. The Board should also ensure that senior management takes the steps necessary to monitor and control cyber risk. The board and senior management should have a good understanding of the authorized institution's cybersecurity posture and latest cybersecurity threat, and fully support and have effective oversight on key cybersecurity initiatives and objectives. Hence, cybersecurity should be very visible at the board level, and cybersecurity reporting should be provided to the board regularly and immediately if there are any material change to the cyber risk. Such reporting should be discussed in the board with appropriate action taken.

4.2. Strategy

4.2.1. *Cybersecurity Strategy*. Cybersecurity strategy should be risk-based with the aim of enhancing cybersecurity posture. It should be reviewed regularly by all business stakeholders, senior management and the board. The strategy should be sufficiently detailed with supporting plans to explain the why, what, how, when for each major initiative.

4.3. Cyber Risk Management

4.3.1. *Embedding cyber risk management into enterprise risk management.* Cyber risk management should be an integral part of the enterprise operational risk management framework. A function should be established to manage cyber risk within the authorized institution. Policies, procedures and controls between cyber risk and other areas of risks should be aligned as necessary.

4.3.2. *Cyber Risk Tolerance.* Authorized institutions should define their cyber risk tolerance with endorsement from board and senior management. Authorized institutions should also perform regular review on the cyber risk tolerance.

4.4. Cyber Resilience Framework

4.4.1. Cyber Resilience Framework consists of the policies, procedures and controls an authorized institution has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces. Authorized institutions should have a cyber resilience framework that clearly articulates how it determines its cyber resilience objectives and cyber risk tolerance, as well as how it effectively identifies, mitigates, and manages its cyber risk to support its objectives. It should be aligned with the authorized institution's organization-wide risk management framework. Such framework should be endorsed by the board.

4.4.2. *Ownership of Cyber Resilience Framework.* Cyber resilience framework and its supporting policies should be owned by senior management who has sufficient knowledge and experience, and the authority to consistently enforce implementation of the framework. The supporting policies should be fully aligned with the cyber resilience framework.

4.4.3. *Scope and availability.* Cyber resilience framework should cover all processes and technology components within the authorized institution. IT and business stakeholders should be engaged to ensure the practicality of the cyber resilience framework and supporting policies throughout the development and review processes. It should be well communicated across the organization as an on-going basis.

4.4.4. *Monitoring of effectiveness.* Formally defined and documented process should be established for measuring, tracking, and monitoring compliance with the cyber resilience framework and supporting policies. Identification, tracking, and monitoring of gap remediation should also be continuously conducted by the risk management function (or equivalent).

4.4.5. *Review and Updates*. Proper review and update should be conducted for the cyber resilience framework and supporting policies under a formal process regularly to address latest cyber threat and to align with industry standards, legal and regulatory requirements. The review process should be performed annually, and more often if a significant cybersecurity event or incident warrants an immediate update.

4.5. Accountability

Accountability and importance of cybersecurity should be clearly understood and accepted within the authorized institution. Roles and responsibilities of cyber risk management should be established with clear reporting line. Authorized institutions should also consider the independence requirement of the reporting line in the management model (such as three lines of defence model). It is important that accountability of cybersecurity management is upheld and relevant staff performance should be regularly assessed against defined roles and responsibilities.

4.6. Resources

4.6.1. *Budget and Resources Allocation*. To support proper implementation of the Cybersecurity measures, authorized institutions should have proper budget and resources allocation (e.g. staffing, cybersecurity tools, external expertise) supporting the execution of Cybersecurity management. In addition, a proper budgeting process should be in place to support regular and ad-hoc funding.

4.6.2. *Qualified Staffing*. Authorized institutions should ensure that the relevant personnel (including board, senior management and staff) with cybersecurity responsibilities have adequate knowledge and experience. Staff with cybersecurity responsibilities should also have relevant qualifications to perform the necessary tasks relevant to his position.

4.7. Third Party Management[7]

4.7.1. *Third Party Management Program*. A third party management program should be established with proper ownership and accountability. The program should cover, but not be limited to, third party risk assessment, third party selection process and third party evaluation. Authorized institutions should establish responsibilities and process for effective incident handling and disaster recovery.

4.7.2. *Risk Assessment.* Third party risk should be covered in the organization-wide risk agenda for senior management’s discussion. Risk assessment should be performed for vendor prior to adoption and regularly for the existing vendor. Cybersecurity and data privacy should be a key area for the assessment.

4.7.3. *Contractual Agreements*. The importance of cybersecurity and data privacy should be communicated to all third parties in formal documents. All third party contractual agreements should include standard clauses concerning security requirements and annual review requirements on third party vendors.

4.8. Audit and Compliance

4.8.1. *Independent Audit Function*. In order to assist the board and senior management to assess and measure the adequacy and effectiveness of the authorized institution’s cyber resilience framework, an independent audit function (or equivalent) with adequate qualification should perform the review and report the finding to the board and senior management. The identified findings and relevant remediation action should be properly tracked.

4.8.2. *Audit Approach.* Authorized institutions should assess regularly the audit approach based on the latest inherent risk profile and cyber threat landscape.

[7] When the third party falls into the scope of outsourcing, authorized institutions should also refer to relevant regulatory requirements regarding outsourcing (see also “Guideline on Outsourcing”).

5. IDENTIFICATION

5.1. IT Asset Management

5.1.1. *IT Asset Management Process.* Authorized institutions should establish an IT asset management process. There should be a centralized and updated asset inventory with critical assets identified, including interconnections with other internal and external systems. Authorized institutions should also understand what business functions and processes that the assets are supporting. Information assets provided to third parties should also be clearly identifiable in the inventory.

5.1.2. *IT Asset Inventory Checking.* Regular checking on the IT asset should be conducted to identify any unregistered assets and unauthorized changes.

5.1.3. *Information Asset Inventory.* To ensure appropriate security measures are implemented to protect critical data, authorized institutions should maintain an inventory of their information assets with proper classification.

6. PROTECTION

6.1. Data Protection

6.1.1. *Data Protection Program.* A data protection program should be established to protect sensitive data at rest, in transit and at use. The program should be reviewed regularly using results of internal or external assessments or audits. Access to sensitive data should be logged and actively monitored for appropriateness. Sensitive data should be encrypted at-rest and in-transit when transmitted across public or untrusted networks. Encryption of sensitive data should also be considered when transmitted across private connections and within the institution’s trusted zones.

6.1.2. *Data Inventories and Data Flows.* Data inventories should include structured and unstructured repositories. Data architecture and sensitive data flows should be maintained, and used to ensure that data protection program provides adequate coverage across the authorized institution and third parties.

6.1.3. *Data Classification*. Authorized institutions should develop a formal policy on how to handle data based on the classification. Appropriate personnel such as the operation and compliance team should review the classification regularly.

6.1.4. *Data Transfer*. Authorized institutions should establish data transfer guidelines that provide clear guidance on security practices of data transfer. There should be measures established to identify and remediate insecure data transfers.

6.1.5. *Data Protection Tools.* Tools (such as Data Loss Prevention solution) should be considered for adoption to detect and block unauthorized transmission of sensitive data.

6.2. Access Control

6.2.1. *Policies for Access Control.* Authorized institutions should formally establish policies for access control. The policy should cover user account management, privileged account management, monitoring, account review and physical access management.

6.2.2. *User Account Management*. Physical and logical access to system should be restricted for individuals who are authorized. Authorized institutions should implement reliable controls such as role-based access, segregation of duties and strong authentication (e.g. multifactor authentication) to restrict system access. Authorized institutions should consider adopting an automatic provisioning and de-provisioning of user access based on changes required. Meanwhile, for changes triggered from employment termination or resignation, authorized institutions should consider adopting automated de-provisioning to be driven by Human Resource system.

6.2.3. *Privileged Account Management.* Authorized institutions should implement strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. All privileged accounts and shared accounts should be centrally managed, and their passwords should be managed using a password vault solution that automatically changes passwords after checkout. Based on a risk-based approach, multifactor authentication should be used for privileged access to high-risk systems and access to sensitive or confidential data.

6.2.4. *Monitoring of User Accounts and Privileged Accounts*. Monitoring of user accounts and privileged accounts should be implemented to detect any unauthorized access. Authorized institutions should consider to incorporate such monitoring into organization-wide security monitoring solution with the use of security event correlation and alerting capabilities.

6.2.5. *Access Reviews.* Authorized institutions should conduct access review on a regular basis to identify any excessive privileges and obsolete accounts to prevent unauthorized access.

6.2.6. *Physical Access Management*. Physical access control should be implemented to prevent unauthorized access to organization assets. Access control mechanisms should be used to monitor the entry or exit points. Physical protection mechanisms should be protected from tampering and should be actively monitored. Sensitive areas should have additional locks or alarms.

6.3. Network Security

6.3.1. *Policies and Processes*. Authorized institutions should establish relevant policies and processes for network security covering areas such as network access management, network protection, configuration management, vulnerability management, etc.

6.3.2. *Network Access Management.* Proper network access control should be implemented and strong authentication should be adopted for critical network asset. Network activities should be properly logged and monitored. All incoming and outgoing third-party connections, and their related trust levels should be properly set, documented and regularly reviewed. Remote access to administrative systems should be restricted. Authorized institutions should also implement controls to prevent unpatched and unauthorized device connecting to the network.

6.3.3. *Network Protection*. Network should be properly protected and segmented. Internal network should be properly segregated into different trust / security zones to mitigate attacks. Network perimeter defense tools (e.g. border router and firewall) should be used. Intrusion detection system (IDS) and intrusion prevention system (IPS) should be adopted and properly configured to detect and block potential intrusions. Authorized institutions should also implement adequate solution to prevent and mitigate disruptive cyber attacks (e.g. Denial-of-service attack). Wireless networks should also be strongly protected by proper encryption and segmentation.

6.3.4. *Configuration Management*. All changes to the network infrastructure should be implemented by following a documented end-to-end change management process and approval. Firewall rules should be adequately configured and preferably administered centrally. The administrative access to the network device should be properly confined and monitored to prevent unauthorized change.

6.3.5. *Vulnerability Management.* Periodic review should be performed that scan the network for security vulnerabilities. Network devices should be regularly patched and kept up-to-date.

6.3.6. *Network Architecture.* Detailed network architecture should be maintained and updated regularly.

6.4. Anti-virus / Anti-malware. Anti-virus and anti-malware tools should be adopted with up-to-date definitions.

6.5. System Development

6.5.1. *System Development Life Cycle (SDLC).* Authorized institutions should establish a formal SDLC process which incorporates the principle of secure development. It should include specific checkpoints to assess security risks and identify mitigation strategies in different phases of the SDLC including systems analysis and requirements definition, systems design, development, integration and testing, acceptance, installation, deployment, maintenance, evaluation, and disposal.

6.5.2. *Secure Coding Practice*. Secure coding practices should be established with reference to industry standard. Vulnerabilities identified from vendor, security tools, penetration testing and vulnerability scanning should be considered when developing and updating such practices.

6.5.3. *Secure Development Environment*. Authorized institutions should consider setting up development environments which have similar security controls implemented in production environment.

6.5.4. *Change Management*. Change management processes should be integrated with baseline configuration standards, such that any technology changes may trigger update of such standards. System change and update should be validated before applied to production.

a) During the system development process, secure configuration and risks associated with the technology components should be considered and assessed against a threat model. Third party components should be evaluated for stability, security and overall risk before they are adopted.

b) During the testing phase, relevant security testing (such as penetration testing, source code review, vulnerability assessment) should be performed before implementing in production environment.

6.5.5. *System Developed by Third Parties*. For system developed by third parties, authorized institutions should also perform review on their security impact similar to the requirement for developing in-house. Authorized institutions should also maintain a list of the third parties service provider and consider implementing relevant security controls as recommended in the Third Party Management.

6.6. Software Security

6.6.1. *Software Acquisition.* Software should be evaluated for security risk before acquisition, and relevant security testing (such as penetration testing) should be performed prior to implementation.

6.6.2. *Continuous Monitoring and Improvement.* Authorized institutions should implement control to prevent unauthorized change to software as recommended in the Detection domain. The software should be continuously tracked for security update. For end-of-life support software, authorized institutions should regularly assess the security impact of continuing the use of such software.

6.7. Patch Management

6.7.1. *Patch Management Process*. Patch management process should be formally defined and documented. Change management controls should be incorporated in the patch management process. Testing, and risk and vulnerability mitigation evaluation should be performed throughout the process. The process should be reviewed regularly to ensure compliance.

6.7.2. *Patch Checking.* Authorized institutions should identify exceptions on configuration and patch handling. Authorized institutions should consider using scanning tools or automated tools for identifying exceptions. Exceptions should be mitigated or resolved in a timely manner or within the defined timeframe.

6.7.3. *Remediation*. Authorized institutions should maintain the requirements for patch management on an on-going basis. Timeframe should be set for patches with different criticality. Remediation plans should be developed for non-compliance, and are tracked and monitored for completion by the defined deadlines.

6.8. Configuration Management

6.8.1. *Baseline Configuration*. Authorized institutions should establish and enforce baseline system configuration and perform review regularly as per industry standard and cyber threat.

6.8.2. *Configuration Change.* Any change to the configuration should follow change management process with proper control and monitoring. Authorized institutions should consider implementing technical solution to prevent unauthorized change of configuration on critical systems.

6.9. Mobile Devices Management

6.9.1. *Mobile Devices Management.* Authorized institutions should establish relevant security controls to protect the use of mobile device (for both corporate and personal device), especially if sensitive data is able to be accessed from mobile device. Checking should be conducted regularly for compliance.

6.9.2. *Wiping of Mobile Devices.* Authorized institutions should implement controls to allow wiping of mobile devices remotely when the device is missing or stolen.

6.10. Physical and Environmental Protection

6.10.1. Authorized institutions should prevent unauthorized damage and interference to their data centres and other information processing facilities. In particular, protection and monitoring controls should be implemented against natural disasters, malicious attack and accidents.

7. **DETECTION**

7.1.1. *Security Monitoring Processes.* Security monitoring processes and procedures should be formally defined and documented, and consistently followed. Documentation should be reviewed and updated to reflect changes in processes or procedures.

7.1.2. *Logging.* Logging should be implemented to enable security monitoring and anomalous activities detection. Logging practice should be formally defined and documented with regular review. The logging practice should include, but not be limited to, types of log to be recorded, retention period, disposal methods, masking requirement of logs, and the frequency of log collection and review. Authorized institutions should have a logging mechanism which enable better security monitoring and log protection.

7.1.3. *Monitoring.* Authorized institutions should take a risk-based approach to monitoring that covers multiple components (e.g., monitoring of the high-risk network, host, privileged access, file-level etc.). Monitoring should be accomplished via automated alerts (e.g., emails, text messages) that are sent to designated response personnel for pre-defined events (e.g., high risk, low likelihood of false positive events). These alerts should be properly monitored and reviewed. Security monitoring reporting should be provided to management and other audiences as required on a regular basis.

7.1.4. *Security Information and Event Management*. Authorized institutions should implement relevant process and tool to effectively perform security monitoring. Authorized institutions should consider adopting tools to consolidate logs from different sources such as application logs, access logs, logs from network devices, access to sensitive data and intelligence feeds from third-party sources and vulnerability scanning results to perform correlation analysis and identify potential security threats. Authorized institutions should also establish detection capability regarding simultaneous attacks. Such intelligence feeds should be regularly updated.

7.1.5. *Security Monitoring Team.* A qualified team (e.g. Security Operation Center) should be dedicated to monitor security events. Roles and responsibilities of security monitoring team members should be formally documented and communicated.

8. RESPONSE AND RECOVERY

8.1. Business Continuity Planning [8]

8.1.1. *Crisis Management Plan.* Authorized institutions should formally develop Crisis Management Plan for handling disruptive and unexpected cyber events. Roles and responsibilities should be included in the Crisis Management Plan. Crisis escalations and incident management protocols should be established and consistently followed.

8.1.2. *Business Continuity Management Program.* Authorized institutions should set up a Business Continuity Management Program and a committee consisting of senior management and relevant stakeholders from business and IT to take the ownership and responsibility of the program. Roles and responsibilities should be fully established and endorsed by the committee. The Business Continuity Management Program framework and policy should be operationalized across the authorized institution.

8.1.3. *Business Impact Analysis.* Business impact analysis, risk assessments and gap analysis should be conducted to update the Business Continuity Management program. Business impact analysis results should be used to prioritize the recovery of services.

[8] Authorized institutions should also refer to the relevant requirements regarding Business Continuity Management (e.g. “Guideline on Business Continuity Management”).

Gap analysis should be conducted to identify the discrepancies between the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and the existing recovery capabilities. Key findings, and threats and vulnerabilities from the gap analysis should be reviewed and acknowledged by the senior management.

8.1.4. *Resources Management.* Teams for business continuity and disaster recovery should be identified, trained and made aware of their roles. Relevant budget should be planned and allocated at least annually to align with the planned Business Continuity Management initiatives as approved by the respective committee.

8.1.5. *Disaster Recovery Plan.* A Disaster Recovery Plan should be established for the authorized institution to recover the IT functions during disaster. Testing plays an important role in identifying the room for improvement in the Disaster Recovery Plan and making stakeholders familiarized with the Disaster Recovery Plan. Disaster recovery drill should be integrated and functional in nature - business, IT and third-party service providers should participate in the drill. The Disaster Recovery Plan should be updated at least annually based on the drill results.

8.2. Incident Management

8.2.1. *Incident Management Program.* Authorized institutions should maintain an incident management program, which provides the visibility to board and senior management, and for their ongoing oversight and support. The program should cover different areas such as incident identification, reporting, classification, handling, notification and recording.

8.2.2. *Incident Management Procedures.* A formal chain of custody procedures (including forms, log, procedures, etc.) should be defined, documented and communicated to all members of the incident response ("IR") team as well as other relevant internal and external stakeholders (e.g., staff, contractors, vendors, suppliers, etc.). Decision criteria should be fully defined and documented and consistently used in the triage process of incidents. Additional procedure to facilitate forensic investigation (e.g. digital evidence handling) should also be considered to support the incident response.

8.2.3. *Incident Classification Matrix.* Incident classification matrix should be established for clear incident classification in order to execute the corresponding handling and reporting procedures. Different scenarios should be taken into consideration during the design of incident classification matrix.

8.2.4. *Incident Communication and Reporting.* Incident communication and reporting requirements should cover both internal and external parties. External reporting requirements (such as regulatory or legal) should be identified, documented and communicated to all responsible parties. Regulatory reporting requirements should also be reviewed by subject matter experts (e.g., compliance, legal, etc.) to ensure accurate interpretation. Specific procedures should be defined to guide actions so that compliance can be achieved and errors or delays can be avoided.

8.2.5. *Reporting to AMCM.* Authorized institutions should report such incident according to the requirement in "Incident Reporting Measures for Major Emergencies".

8.2.6. *Testing.* Authorized institutions should perform regular testing of their incident response plan. When there is significant change in the incident response plan, testing should be performed to ensure that the change does not affect business availability and still meet the business needs. Authorized institutions should consider involving critical third parties in the testing. The results of the testing should be used to improve the incident response plan.

8.2.7. *Incident Management Team and Resources.* A cross-functional IR team should be assembled to ensure the right skills and expertise exist to support incidents in scope of the program. The team should have relationships with functional authorities and industry groups to leverage when needed. The board of the authorized institution should take the final accountability for all incidents. Roles and responsibilities should be reviewed regularly to identify and fill gaps in capabilities.

8.2.8. *Up-to-date Incident Management Programme.* Authorized institutions should keep the incident management programme up-to-date with emerging threats and technologies. Recent cases of cyber incidents and attacks could be used to continuously improve the programme. Apart from the program, supporting components of the program such as testing scenario and resource arrangement should be updated.

8.2.9. *Incident Response*. Incident response processes should interface with other parts of the authorized institution (e.g., Crisis Management team) to ensure timely remediation and communication with internal and external stakeholders.

9. TESTING

9.1. Testing Programme

9.1.1. Authorized institutions should establish a testing programme to validate the effectiveness of their cybersecurity management on a regular basis. Relevant and latest cyber threat intelligence should be employed when designing (or updating) the testing programme. When designing (or updating) such programme, authorized institutions should involve key stakeholders such as board and senior management and relevant business line management, and consider the involvement of external stakeholders such as critical third-party. The condition of triggering and frequency of such testing should be identified. Authorized institutions should also establish the set of measures so that their production systems will not be affected during the testing. The level of independence required of the testing should be determined and the testing programme should enable ongoing improvement of cybersecurity management.

9.2. Testing Methodologies and Practices

9.2.1. *Vulnerability Assessment*. Authorized institutions should perform vulnerability assessment regularly to identify and assess security vulnerabilities in the systems. Processes should be established to prioritise and remediate issues identified in vulnerability assessment and validate the remediation.

9.2.2. *Penetration Testing*. Authorized institutions should perform penetration testing on their assets such as applications, infrastructure, internal and external network, and endpoint devices, which should simulate actual attack scenario on the systems, to identify vulnerabilities in business processes and technical controls. The testing should be performed on the asset before they are placed into production and after major changes to the asset. There should be a risk-based schedule to test existing assets. The scope of the testing on existing assets should be compared against an established asset inventory to ensure coverage. Apart from the white-box[9] penetration testing approach, other testing approaches such as black-box[10] and grey-box[10] style testing can also be considered. Results of the penetration testing should be used to enhance the system development as part of the secure coding practice and cybersecurity management.

9.2.3. *Red Team Testing*[10]. Authorized institutions should consider adopting red team testing to simulate adversarial attempt to compromise their business process to obtain a comprehensive assessment of the security capabilities of the information system and organization, including the potential vulnerabilities and the respective effectiveness of detection and response.

9.2.4. *Scenario-based Testing*. Scenario-based testing, such as incident response testing should be conducted to test the ability of staff and processes to respond to different scenarios in order to achieve stronger operational resilience.

9.3. *Remediation Management Process*. Authorized institutions should have a formal remediation management process for handling the vulnerabilities identified from the testings stated in Section 9.2. A mechanism to centrally track the remediation of vulnerabilities through their lifecycle should also be established. Ownership for vulnerability remediation should be assigned and recorded properly. Re-assessment of all remediated vulnerabilities should be performed before they are considered closed. The status of the remediation should be reported regularly to senior management.

[9] White-box, black-box and grey-box testing: White-box Testing - A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Black-box Testing – It is in contrast to the white-box testing, in which the tester has no knowledge at all. Grey-box Testing – It is a test methodology in between white-box and black-box, in which the tester has some knowledge of the assessment object.

[10] Red team exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.

9.4. *Qualified Tester*. Authorized institutions should ensure that the testing is conducted by tester with adequate knowledge, experience and qualification[11].

10. SITUATIONAL AWARENESS

10.1. Situational Awareness of Authorized institution

10.1.1. *Threat Intelligence.* Authorized institutions should identify cyber threats that could materially affect their ability to perform or to provide services as expected, or that could have significant impact on its ability to meet its own obligations or have knock-on effects within its ecosystem. Authorized institutions should consider threats to the confidentiality, integrity, availability of their business processes and data, and to their reputation that could arise from internal and external sources. Threats from cyber events which are considered unlikely to occur or have never occurred in the past should be considered. Such analysis should be performed regularly of which the results should be applied to the authorized institution’s cybersecurity posture at the strategic, tactical and operational levels.

10.2. Situational Awareness of Staff

10.2.1. *Security Awareness Program.* Authorized institutions should develop a security awareness program to enhance the security awareness of their staff members. Program should be designed with different focus for different target groups covering new and existing staff. Apart from the traditional security subject matters, authorized institutions should continuously enhance the program, taking into consideration the subject matters such as newly developed technology and recent cyber-attacks. Authorized institutions should also consider requiring third parties which handle and/or process personal information or other sensitive data to complete such program.

[11] Refer to Appendix A for the example of professional cybersecurity qualifications on penetration testing and red team testing.

10.2.2. *Effectiveness of the Program.* Authorized institutions should measure the effectiveness of the cybersecurity awareness program. The completion of training should be tracked to ensure compliance. Apart from traditional way of measuring the effectiveness (e.g. training quiz), authorized institution may consider to periodically send out simulated phishing emails, or use other appropriate methods, in testing the awareness of staff.

11. **LEARNING AND EVOLVING**

11.1. Ongoing Learning

11.1.1. *Staff competence and training.* The cybersecurity function of the authorized institution should be adequately staffed and they should have sufficient knowledge and skills to execute their responsibilities. Cybersecurity staff should be trained regularly to keep their knowledge and skill level up-to-date with emerging threats, trends, and technologies.

11.2. Continuous Benchmarking

11.2.1. *Cybersecurity Metrics.* Cybersecurity metrics should be established to aid the authorized institution in understanding the effectiveness of cyber resilience framework and how the framework can support the cyber risk management. Such metrics should allow trend analysis. The use of cybersecurity metrics should allow institution to identify gap in the cyber resilience framework and achieve continuous improvement toward the cyber resilience objective.

11.2.2. *Reporting to Board and Senior Management.* Cybersecurity metrics, updates, and issues should be actively discussed at the Board and Senior Management level on a regular basis. The Board should have a good understanding of the authorized institution 's cybersecurity posture, and actively provides input into the metrics. Strategic level metrics should be developed and presented to management regularly, especially to the Board and Senior Management. The Board and Senior Management should have a good understanding of the Cyber Resilience Framework at a strategic level, through the metrics. Feedback on the metrics in demonstrating strategic security posture should be obtained regularly, and incorporated into improving the metrics program.

11.2.3. *Risk assessment on Cybersecurity Management.* Authorized institutions should conduct risk assessment on cybersecurity management at least every two years or when there are substantial changes which may affect the cyber risk profile. The objective of the risk assessment is for the authorized institution to identify cyber risk and non-compliance issues, and to assess the level of change to the cyber risk profile. The risk assessment should be performed by person(s) with the necessary capabilities who can be internal staff or external party. The results should be approved by senior management and the report should be submitted to AMCM upon request.

11.2.4. *Independent Assessment on Cybersecurity Management.* The independent assessment should, at a minimum, cover paragraphs 4 to 11 of this Guideline and be performed upon notification from AMCM or if the result of the risk assessment as mentioned in 11.2.3 indicates that an independent assessment is necessary. The person(s) performing the independent assessment should have, and be able to demonstrate, the necessary expertise[12] in the relevant fields. He/she should be independent from the parties that develop or administer the system and should not be involved in the operations to be reviewed or in selecting or implementing the relevant control measures to be reviewed. He/she should be able to report findings freely and directly to the authorized institution’s senior management. As long as the assessor meets the above criteria, he/she can be internal staff (e.g. internal auditors) or external party (e.g. an external auditor or other third-parties service providers). The results should be approved by senior management and the report should be submitted to AMCM which should include at least the following items:

a) time of assessment;
b) scope and approach adopted, including descriptions of the system components, internal networks and network equipment that are covered;
c) the assessors’ findings and recommendations; and

[12] Refer to Appendix A for the example of professional cybersecurity qualifications on independent assessment on cybersecurity management.

d) management responses.

Self-assessment as mentioned in 11.2.3 is not required in the year when independent assessment is performed.

11.3. Reference to Industry Standards and Practices

11.3.1. Authorized institutions could refer to different industry standards and practices as a benchmark to evaluate and enhance their cybersecurity controls.

12. SUPERVISORY APPROACH

12.1. The AMCM expects authorized institutions to develop and implement effective cybersecurity management that is consistent with the above-mentioned principles and key processes.

12.2. While this guideline does not dictate the means or specific technologies to implement relevant control, the AMCM expects authorized institutions to implement relevant controls or demonstrate effective means to fulfil such controls in accordance to the cyber risk profile of the authorized institution. Authorized institutions should consider the following area when evaluating their cyber risk profile:

(a) Technologies and Connection Types

(b) Delivery Channels

(c) Online / Mobile Products and Technology Services

(d) Organizational Characteristics

(e) External Threats

12.3. In cases which the authorized institutions are branches of overseas incorporated banks adopting the support from head / regional office to execute the roles and responsibilities of cybersecurity management, they are still expected to demonstrate that such approach can fulfill the requirement and does not undermine the cybersecurity management of the authorized institution. Depending on the circumstances, authorized institutions should take note that the responsibilities of Governance may still require branches' local management for execution.

12.4. Prior to the launch of the relevant services or major enhancements to existing system or services, authorized institutions are expected to have adequate cybersecurity management in accordance to this Guideline, or have completed relevant remediation if there are any major non-compliance / cybersecurity incident.

12.5. The AMCM will, in the course of its onsite examinations and offsite reviews, determine as appropriate the adequacy of authorized institutions' cybersecurity management based on the requirements set out in this Guideline. Authorized institutions are expected to comply with this Guideline as soon as practicable.

APPENDIX A: REFERENCE ON PROFESSIONAL QUALIFICATIONS

Independent Assessment on Cybersecurity Management

- ISACA CSX Fundamentals Certificate
- ISACA CSX Practitioner Certificate (CSX-P)
- ISACA Certified Information Systems Auditor (CISA)
- ISACA Certified Information Security Manager (CISM)
- ISACA Certified in Risk and Information Systems Control (CRISC)
- ISACA Certified in the Governance of Enterprise IT (CGEIT).
- ISC^2 Certified Information Systems Security Professional (CISSP)

Penetration Testing / Red Team Testing

- CREST Certified Simulated Attack Manager
- CREST Certified Simulated Attack Specialist
- CREST Certified Infrastructure Tester
- CREST Certified Web Applications Tester
- GIAC Penetration Tester (GPEN)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Exploitation Expert (OSEE)
- Offensive Security Web Expert (OSWE)
- Offensive Security Certified Professional (OSCP)

APPENDIX B: REFERENCES ON INDUSTRY STANDARDS AND PRACTICES

- Control Objectives for Information and Related Technology (COBIT)
  - http://www.isaca.org/cobit/pages/default.aspx
- SANS Top 20 Critical Security Controls (CSC)
  - https://www.sans.org/critical-security-controls/
- Information Security Forum – Standard of Good Practice for Information Security
  - https://www.securityforum.org/
- ISO/IEC 27001 Information security management
  - https://www.iso.org
- ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls
  - https://www.iso.org
- ISO/IEC 27035, Information technology – Security techniques – Information security incident management
  - https://www.iso.org