澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

Circular No. 017/B/2023-DSB/AMCM

Date: 11/12/2023

Guideline on Technology and Cyber Risk Management

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 8 of Law no. 13/2023 (Financial System Act, hereafter referred to as FSA), establishes the following:

1. INTRODUCTION

1.1. The technology and cyber risk landscape of the financial sector has been rapidly transforming. Many financial institutions are embracing digitalization to increase their operational efficiency and deliver better services to customers. While this is bringing significant benefits to the financial ecosystem, it is also increasing financial institutions' exposure to a range of technology and cyber risks. These risks are increasing not only because of the growing complexity of the underlying technologies being used to support operation and financial services, but also because of the increasingly sophisticated techniques being adopted by cyber threat actors. Financial institutions should therefore take proactive steps to understand their exposure to technology and cyber risks, and to put in place effective controls to protect their organizations and customers.

1.2. This Guideline provides authorized institutions[1] with a set of technology and cyber risk management principles and best practices, designed to support authorized institutions in developing greater resilience to technology and cyber risks. Since both the technologies adopted by the financial industry and the related cyber threats are evolving rapidly, the recommendations in this Guideline should not be considered as final or definitive. Apart from existing regulatory requirements and guidelines[2], authorized institutions should always take into account the latest industry standards and practices[3] to ensure that their technology and cyber risk management practices are adequate and consistent with the nature and scale of their business.

[1] Credit institutions and the institutions mentioned in this Guideline are collectively referred to as "authorized institutions".
[2] These include (but not limited to) the "Guideline on Risk Management of Electronic Banking", the "Guideline on Outsourcing", the "Guideline on Business Continuity Management" and the Incident Reporting Measures for Major Emergencies.
[3] Refer to Appendix B for references of industry standards and practices.

1.3. This Guideline sets forth the key principles for managing the risks associated with cybersecurity and the adoption of technology. All authorized institutions are expected to adopt the key principles, which will assist them in establishing a sound and robust technology and cyber risk management process. The Guideline is applicable to the following financial institutions authorized under the provisions of the FSA and specific laws and regulations other than the FSA:

(a) credit institutions that are either locally incorporated or are branches of overseas banks in Macao;
(b) financial companies;
(c) cash remittance companies;
(d) assets management companies;
(e) investment fund management companies;
(f) other financial institutions.

1.4. In this Guideline, the AMCM has taken into account the risk management principles and sound practices found in similar technology and cyber risk management standards, guidelines and frameworks being used by other regulatory authorities as well as international standards[4]. Domains similar to those used in such standards, guidelines and frameworks have been adopted here to organize related requirements. Authorized institutions are encouraged to familiarize themselves with the main principles of these other documents.

2. RISK POSTED BY AND ASSOCIATED WITH TECHNOLOGY

[4] For example:

- "Guidance on cyber resilience for financial market infrastructures" (June 2016), issued by the Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions (CPMI-IOSCO)
- "Fundamental elements of cybersecurity for the financial sector" (October 2016), issued by the Group of Seven (G7)
- "Technology and Cyber Risk Management" (November 2021), issued by the Office of the Superintendent of Financial Institutions (OSFI)
- "Cybersecurity assessment tool" (May 2017), issued by the United States Federal Financial Institutions Examination Council (FFIEC)
- "Framework for improving critical infrastructure cybersecurity" (April 2018), issued by the National Institute of Standards and Technology (NIST) of the United States
- "Cyber resilience oversight expectations for financial market infrastructures" (December 2018), issued by the European Central Bank
- "EBA Guidelines on ICT and security risk management" (November 2019), issued by the European Banking Authority (EBA)

2.1. Technology and cyber risk refer to risks arising from the use of information technology (IT) and the Internet. These risks include failures or breaches of IT systems, applications, platforms or infrastructure, which can result in data loss, financial loss, disruptions to financial services or operations, or reputational harm to an authorized institution.

2.2. As the use of technology for the provision of financial services and support of operations becomes more prevalent, authorized institutions need to strengthen their technology and cyber resilience to avoid operational disruptions and maintain public confidence in the institution and the financial system. The growing sophistication of cyber threats also demands increased vigilance on the authorized institutions, as well as strengthened capability to respond to emerging threats. Critical and essential financial services should always be available to customers, and customer data should always be adequately protected.

2.3. Inappropriate usage of authorized institutions' information technology resources may have significant risk implications. These could include, but not limited to: (1) strategic risks resulting from poor decisions on technology-related investments; (2) operational risks caused by unauthorized access or disruptions to technology resources that support mission-critical banking services; and (3) reputational and legal risks arising from material security breaches or the unavailability of computer systems needed to process customer information or transactions.

2.4. The board of directors is ultimately responsible for understanding the risks faced by an authorized institution and ensuring they are properly managed; while the senior management is accountable for designing and implementing a risk management system approved by the board. To this end, the senior management should establish an effective technology and cyber risk management framework. This should normally include an IT governance structure, a continuously updated technology and cyber risk management process, and implementation of sound practices in respect of IT controls.

3. STRUCTURE OF THE GUIDELINE

3.1. This Guideline is divided into six domains. Each domain should be addressed by an authorized institution as part of its technology and cyber risk management process. The domains are summarized below, and discussed in more detail in Sections 4 to 11.

a) *Technology and Cyber Risk Management Framework.* Having an effective technology and cyber risk management framework allows an authorized institution to better understand and manage its risk profile. Risk management involves identifying risks, assessing and monitoring risk exposures, and taking steps to mitigate the exposures with the necessary resources on an ongoing basis. Once such a framework has been established, internal controls can be embedded into daily operations to manage exposures to technology and cyber risks effectively and efficiently. The requirements are further elaborated in Section 4.

b) *Governance and Strategy.* Sound governance, guided by a clear technology and cyber strategy, is an essential part of good technology and cyber risk management. The governance process should define an authorized institution's technology and cyber resilience objectives, and set out the relevant requirements on people, processes and technology for achieving the objectives. The board[5] and senior management should have clearly defined roles and responsibilities, and there should be a good culture in place that recognizes the importance of technology and cyber risk management. The authorized institution should establish, implement and regularly enhance its governance approach to managing technology and cyber risks. These requirements are further elaborated in Section 5.

c) *IT Project Management and System Development.* Having consistent IT project management practices allows an authorized institution to monitor its projects effectively and to ensure that outcomes are aligned with its business objectives and are within the scope of its risk appetite. A System Development Life Cycle (SDLC) framework should be implemented to ensure the secure development, acquisition and maintenance of IT systems that will perform as expected in support of the institution's business objectives. Security practices should be embedded into the SDLC process to minimize system vulnerabilities and reduce the attack surface. These requirements are further elaborated in Section 6.

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

d) *IT Service Operations.* Effective IT service operation controls ensure the stability of the IT production and backup environments. An authorized institution should establish proper governance frameworks, policies, processes and procedures for its IT service operations, with the aim of maintaining and improving their operations security, stability and efficiency in line with its business needs. These requirements are further elaborated in Section 7.

e) *Cybersecurity.* Strong cyber resilience is critical for maintaining public trust and confidence in financial services. Without effective security controls over systems and processes, the confidentiality, integrity and availability of data and systems could be compromised. An authorized institution should implement appropriate safeguards to ensure the uninterrupted delivery of critical services, and to contain the impact of any potential cybersecurity event. These requirements are further elaborated in Section 8.

f) *Response and Recovery.* An authorized institution should be able to operate on an ongoing basis, and to limit losses in the event of severe business disruption. It should therefore have plans for responding to potential failure scenarios, including cybersecurity events, as well as plans for ensuring the resilience and recovery of any services impaired by disruptive events. These requirements are further elaborated in Section 9.

4. TECHNOLOGY AND CYBER RISK MANAGEMENT FRAMEWORK

4.1. Risk Management Framework

4.1.1. *Technology and cyber risk management framework.* A technology and cyber risk management framework should be established. This should consist of a set of technology and cyber risk management policies, procedures and controls, and should include clearly defined roles, responsibilities and reporting lines. The framework should articulate how the authorized institution determines its technology and cyber risk management objectives and risk tolerance, and how its technology and cyber risk management process supports its business objectives. This framework and any subsequent modification to this framework should be approved by the board.

4.1.2. *Technology and cyber risk management embedded in enterprise risk management.* The objectives, policies, procedures and controls that constitute the technology and cyber risk management framework should be aligned with the authorized institution's enterprise-wide risk management practices. The technology and cyber risk management framework should also be an integral part of its enterprise operational risk management framework.

4.1.3. *Scope and availability*. The technology and cyber risk management 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 technology and cyber risk management framework and supporting policies across the risk management processes. The framework should be clearly and regularly communicated across the organization.

4.1.4. *Review and Updates.* The adequacy and effectiveness of the technology and cyber risk management framework and supporting policies should be reviewed and updated regularly, taking into account the changing business and IT environments and the evolving cyber threat landscape.

4.2. Risk Management Process

4.2.1. *Technology and cyber risk management process.* A formally defined and documented technology and cyber risk management process should be established that at a minimum encompasses risk identification, risk assessment, risk mitigation, and risk monitoring, review and reporting.

a) *Risk identification.* Any threats and vulnerabilities applicable to the authorized institution's IT environment should be identified for all processes and assets supporting its business and operations, including assets that are maintained or supported by third party service providers and related parties.

b) *Risk assessment.* An assessment of the potential impact and consequences of threats to and vulnerabilities of the overall business and operations should be carried out. A set of criterion for measuring and determining the likelihood and impact of the risk scenarios should be established, in order to prioritize the technology and cyber risks faced.

c) *Risk mitigation measures.* Risk mitigation measures should be implemented to align with the criticality of the authorized institution's IT assets and its risk tolerance level. If there are residual risks that cannot be fully eliminated, re-assessment should be carried out after measures have been put in place to ensure these risks have been reduced to an acceptable level.

d) *Monitoring, review and reporting*. The authorized institution should establish a process for monitoring the operating effectiveness of IT controls against identified risks. A risk register should be established and maintained by the authorized institution to define the technology and cyber risks that it encounters. Any significant risks in the risk register should be closely monitored and reported to the board and the senior management, and the frequency of the reporting should be commensurate with the level of risk. A risk metric should be developed to quantify and report the exposures of significant technology and cyber risks.

5. GOVERNANCE AND STRATEGY

5.1. Board and Senior Management

5.1.1. *Board and Senior Management Responsibilities.* The primary responsibility for technology and cyber risk management rests with the board and senior management of an authorized institution. The board should establish and approve the authorized institution's technology and cyber risk appetite profile and tolerance by defining the level of risk it is willing to assume. The board should also ensure that senior management takes all necessary steps to monitor and control risks. The board and senior management should have a good understanding of the authorized institution's IT environment and latest cybersecurity threats, and should fully support and effectively maintain oversight over key technology and cyber risk management initiatives and objectives. Hence, technology and cyber risk matters should be very visible at the board level, and risk reporting (e.g. technology and cyber risk metrics) should be made to the board regularly and immediately if there is any material change to risk register for the board discussion and to take appropriate action.

5.1.2. *Ownership of the Technology and Cyber Risk Management Framework.* Senior management with relevant and sufficient knowledge and experience should be given ownership of the

technology and cyber risk management framework and its supporting policies which aligned with the framework. These personnel should also have the authority to consistently enforce implementation of the framework and policies. Appropriate governance structures and processes should be established, with well-defined roles and responsibilities, and clear reporting lines across organizational functions.

5.1.3. *Technology and Cyber Risk Management Functions*. At a minimum, the board and senior management should establish a function (or a dedicated group) to support and implement the technology and cyber risk management process within the authorized institution. This function or group should continuously carry out risk identification, risk assessment, and the tracking and monitoring of risk mitigation measures.

5.2. Strategy

5.2.1. *Technology and Cyber Strategy*. A technology and cyber strategy should set goals and objectives that are measurable and evolve with changes in the authorized institution's IT and cyber environments. The strategy should be sufficiently detailed and include supporting information explaining the reasons for each major initiative. The strategy should take into account the potential risks associated with the authorized institution's short-term and long-term plans (e.g. new business initiatives, organizational changes, technology adoption, cybersecurity planning, etc) and fits within the enterprise-wide risk management strategy. The strategy should be reviewed regularly by the board and senior management.

5.2.2. *Risk Appetite and Risk Tolerance*. The risk appetite and risk tolerance levels for technology and cyber risks that the authorized institution is willing and able to assume should be clearly defined, and this should be endorsed by the board and senior management. The risk appetite profile and tolerance levels should be regularly reviewed.

5.3. Resources

5.3.1. *Budget and Resources Allocation*. To support effective implementation of technology and cyber risk management measures, there should be a proper budget and resources allocation process (e.g. for areas such as staffing, cybersecurity tools, and

external expertise). The proper budgeting process should be able to support regular and ad-hoc funding requirements.

5.3.2. *Qualified Staffing*. The authorized institution should ensure that all personnel with technology and cyber risk management responsibilities (whether board members, senior management or staff) have adequate knowledge and/or experience. Staff holding such responsibilities should also have relevant qualifications and/or experience for performing their respective tasks.

5.4. Third Party Management[6]

5.4.1. *Third Party Management Programme.* A third party management programme should be established with proper ownership and accountability. The programme should cover, but not be limited to, third party risk assessment, third party selection process, and third party evaluation. Responsibilities and processes for effective incident handling and disaster recovery should be established.

5.4.2. *Risk Assessment.* Third party risk should be included in the enterprise-wide risk agenda for discussion by senior management. Risk assessment should be performed on new vendors, and carried out regularly on existing vendors, with a special focus on cybersecurity and data protection and privacy.

5.4.3. *Contractual Agreements*. The importance of technology and cyber risk management (e.g. cybersecurity and data protection and 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.

5.5. Audit and Compliance

5.5.1. *Independent Audit Function*. To help the board and senior management assess the adequacy and effectiveness of the authorized institution's technology and cyber risk management framework, an independent audit function (or equivalent) with adequate qualifications and experience should perform relevant reviews and report the findings to the board and senior

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

management. Any issues identified, along with relevant remediation actions, should be properly tracked and reported.

5.5.2. *Audit Approach.* The technology and cyber risk audit plan should document a set of auditable areas, including IT processes, functions, and information systems. The frequency of assessment of each of the auditable areas should be determined using a risk-based approach, with reference to system criticality and confidentiality of information. The authorized institution's audit approach should be regularly reviewed in light of its latest inherent risk profile and the changing cyber threat landscape.

5.6. IT Asset Management

5.6.1. *IT Asset Management Process*. An IT asset management process should be established. This should be a centralized and regularly updated asset inventory that identified critical assets, including interconnections with other internal and external systems. The authorized institution should also understand what business functions and processes are supported by the IT assets. In addition, ownership of and responsibilities in managing the IT assets, including IT assets managed by third parties, should also be clearly defined in the inventory.

5.6.2. *IT Asset Inventory Checking*. Regular checking of IT assets should be conducted to identify any unregistered assets or unauthorized changes.

5.6.3. *Information Asset Inventory.* The authorized institution should at least define the ownership of its critical information assets, which include customer and internal data, hardware and software, and assign the respective roles and responsibilities for managing them. The owners should work with related functions (e.g. IT, compliance, audit etc.) to ensure appropriate security measures and controls are in place to protect critical data. An inventory of information assets with proper classification and corresponding owners should be maintained and regularly reviewed.

5.7. Situational Awareness of Authorized Institutions

5.7.1. *Situational awareness and information sharing*. The authorized institution should maintain continuous situational awareness of the cyber threat landscape (e.g. emerging cyber threats against financial services industry or organizations in Macau) that applies

to its IT and information assets. This could involve, for instance, participating in industry threat intelligence and information sharing forums and subscribing to timely and reputable threat information sources for information on areas such as: emerging threats, attack techniques, vulnerabilities and indicators of compromise. Cyber threat intelligence sharing could also include sharing with relevant domestic authorities. An authorized institution should timely exchange threat intelligence to prevent cyber attacks, to enhance its own technology and cyber resilience and that of the broader financial sector.

5.8. Situational Awareness of Staff

5.8.1. *Situational awareness programme*. A situational awareness programme should be developed to enhance the security awareness of the authorized institution's staff members. The programme should be designed with different focuses for different target groups, including both new and existing staff. Apart from including traditional security topics, the programme should also include topics such as newly developed technology and attack tactics, techniques and procedures (TTPs) adopted by threat actors. The authorized institution should also consider requiring third parties that handle and/or process personal information or other sensitive data to complete such programme.

5.8.2. *Effectiveness of the Programme*. The effectiveness of the authorized institution's situational awareness programme should be measured. Authorized institution should track to ensure all level of staff, including the third parties, have completed the training. Apart from using traditional means to measure its effectiveness (e.g. training quizzes), simulated phishing emails or other appropriate methods, could be used to test staff awareness.

5.8.3. *Staff competence and training*. The relevant technology and cyber risk management functions of the authorized institution should be adequately staffed. These staff should undergo regular training to ensure their knowledge and skill levels remain up to date in the face of emerging threats, trends, and technologies.

6. IT PROJECT MANAGEMENT AND SYSTEM DEVELOPMENT

6.1. IT Project Management

6.1.1. *IT Project Management.* IT related projects should be governed by an enterprise-wide project management framework approved by the Board. The IT project management framework should set out the standardized approach for managing projects that used technology (e.g. roles and responsibilities, time and resources management, quality assurance, etc.), and the necessary risk controls in managing technology and cyber risk throughout the project lifecycle. Project performance and associated risks should be measured, monitored, mitigated and periodically reported on an individual and portfolio basis.

6.2. System Development Life Cycle

6.2.1. *System Development Life Cycle (SDLC).* A formal SDLC process incorporating the principle of secure development should be established. This should include specific checkpoints to assess security risks and identify mitigation strategies in different phases of the SDLC, including systems analysis and requirement definitions, system design, development, integration and testing, acceptance, installation, development, maintenance, evaluation, and disposal.

6.2.2. *Secure Coding Practice.* Secure coding practices should be established that are in line with industry standards. In developing and updating coding practices, vulnerabilities identified by vendors, security tools, penetration testing and vulnerability assessment should be taken into account.

6.2.3. *Secure Development Environment.* The authorized institution should consider setting up a development environment that has security controls similar to those of its production environment.

6.2.4. *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) In the system development process, secure configuration and risks associated with the technology components should be considered and assessed against different cyber threat scenarios. Third-party components should be evaluated for

stability, security and overall risk before they are implemented.

b) During the testing phase, relevant security testing (such as penetration testing, source code review, and vulnerability assessment) should be performed before any system and component is implemented in the production environment.

6.2.5. *Secure Development by Third Parties.* Reviews should be performed on the security impact of systems and components developed by third parties, just as for systems developed in-house. Authorized institutions should also maintain a list of the third parties service providers and consider implementing relevant security controls as recommended in the Third Party Management in Section 5.4. The authorized institution could consider including in the contracts an escrow agreement with the third parties for critical systems, specifying circumstances which would allow it access to the source code of the systems, so as to minimize service disruption when the third parties were unable to provide support and services.

6.3. Software Security

6.3.1. *Software Acquisition.* Software should be evaluated for security risks before acquisition, and relevant security testing (such as penetration testing and vulnerability assessment) performed prior to its implementation.

6.3.2. *Continuous Monitoring and Improvement.* Controls should be implemented to prevent unauthorized changes to software. The software should be continuously tracked for security updates. In the case of end-of-support or end-of-life software, the security impact of its ongoing use should be regularly assessed.

7. IT SERVICE OPERATIONS

7.1. Access Control

7.1.1. *Policies for Access Control.* Formal policies for access control should be established. The policies should cover user account management, privileged account management, monitoring, account review, remote and physical access management.

7.1.2. *User Account Management*. Physical and logical access to a system and device should be restricted to authorized individuals. Reliable

controls should be implemented to restrict system access, such as role-based access, segregation of duties and strong authentication (e.g. multi-factor authentication). The authorized institution should consider adopting the automatic provisioning and de-provisioning of user access based on user access changes required. For changes triggered by employment termination or resignation, it should consider adopting automated de-provisioning, driven by its system (for instance, the Human Resource system).

7.1.3. *Privileged Account Management.* Strong controls should be implemented over privileged system access by strictly limiting and closely supervising all staff having elevated system access entitlement. 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. Multi-factor authentication should be adopted for privileged access to critical systems and for access to sensitive or confidential data.

7.1.4. *Monitoring of User Accounts and Privileged Accounts.* User accounts and privileged accounts should be monitored for unauthorized access. An authorized institution should consider incorporating such monitoring into an enterprise-wide security monitoring solution with security event correlation and alerting capabilities.

7.1.5. *Access Reviews.* Reviews should be regularly conducted to identify any excessive privileges and obsolete accounts to prevent unauthorized access.

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

7.1.7. *Remote Access Management*. Remote access refers to users connecting to the authorized institution's internal network via external or internet access. In such cases, strong authentication, such as multi-factor authentication should be enforced to prevent unauthorized access. Secure encryption should also be adopted to

protect the remote access session against network sniffing and eavesdropping.

7.2. Patch Management

7.2.1. *Patch Management Process*. A patch management process should be formally defined and documented, and should incorporate change management controls. Testing, and risk and vulnerability mitigation evaluation should be performed throughout the process. The process should be reviewed regularly to ensure compliance.

7.2.2. *Patch Checking.* Exceptions on configuration and patch handling should be identified, for instance by regularly using scanning tools or automated tools. Exceptions should be mitigated or resolved in a timely manner or within a defined timeframe.

7.2.3. *Remediation*. Requirements for patch management should be maintained and regularly updated. Timeframes should be set for patches with different levels of criticality. Remediation plans should be developed for non-compliance, to be tracked and monitored for completion by defined deadlines.

7.3. Configuration Management

7.3.1. *Baseline Configuration*. A baseline system configuration should be established and enforced, and regular reviews be performed in the light of industry standards and cyber threat levels.

7.3.2. *Configuration Change.* Any change to the configuration should follow the change management process, and include proper controls and monitoring. An authorized institution should consider implementing a technical solution to prevent unauthorized changes to the configuration of its critical systems.

7.4. Mobile Devices Management

7.4.1. *Mobile Devices Management.* Relevant security controls should be established over the use of mobile devices (both corporate and personal devices). Before allowing a mobile device access to the authorized institution's internal network or systems, measures such as integrity scanning, mobile device management (MDM) solution, remote software version/patch validation, or other appropriate

methods should be implemented to ensure the mobile device is secure and has not been jailbroken, rooted or compromised.

7.4.2. *Wiping of Mobile Devices.* Controls should be implemented allowing mobile devices to be wiped remotely if they go missing or are stolen.

7.5. Physical and Environmental Protection

7.5.1. Protection should be in place against damage and interference to the authorized institution's data centres or other information processing facilities. In particular, protection and monitoring controls should be implemented to protect against natural disasters, malicious attacks, and accidents.

8. **CYBERSECURITY**

8.1. Network Security

8.1.1. *Policies and Processes*. Policies and processes for network security should be established, covering areas such as network access management, network protection, configuration management, and vulnerability management.

8.1.2. *Network Access Management.* Proper network access controls should be implemented, and strong authentication adopted for critical network assets. Network activities should be properly logged and monitored. All incoming and outgoing third-party connections, and their related trust levels, should be properly defined, documented and regularly reviewed. Remote access to administrative systems should be restricted. Controls should also be implemented to prevent unpatched and unauthorized devices from connecting to the network.

8.1.3. *Network Protection*. Networks should be properly protected and segmented. The internal network should be segregated into different trust / security zones to protect against attacks, and network perimeter defence tools (e.g. border routers and firewalls) should be used. An intrusion detection system (IDS) and an intrusion prevention system (IPS) should be adopted and properly configured to detect and block potential intrusions. Solutions should be implemented to effectively prevent and mitigate

disruptive cyber attacks (e.g. denial-of-service attacks). Wireless networks should be strongly protected with proper encryption and segmentation.

8.1.4. *Configuration Management*. All changes to the network infrastructure (including system configurations) should follow a documented end-to-end change management process with proper testing and approvals. This process should evaluate whether the proposed changes might affect operational activities or introduce security risks. Firewall rules should be adequately configured and preferably administered centrally. Administrative access to the network should be properly confined and monitored to prevent unauthorized changes.

8.1.5. *Vulnerability Management.* Periodic scans of the network for security vulnerabilities should be performed. Network devices should be regularly patched and kept up to date.

8.1.6. *Network Architecture.* Full details of the network architecture should be documented, and regularly updated.

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

8.2. Data Security

8.2.1. *Data Protection Programme.* A data protection programme should be established to protect sensitive data at rest, in transit and in use. The programme should be reviewed regularly in the light of internal or external assessments and audits. Access to sensitive data should be logged, and actively monitored for appropriateness. Sensitive data should be encrypted at rest and in transit if it is transmitted across public or untrusted networks. In addition, encryption or other data protection measures should be adopted or implemented when sensitive data is transmitted across private connections and within the institution's trusted zones.

8.2.2. *Data Inventories and Data Flows.* Data inventories should include structured and unstructured repositories of data. Data architecture and sensitive data flows should be documented, and this information should be used to ensure that the data protection programme provides adequate coverage for both the authorized institution and third parties.

8.2.3. *Data Classification*. A formal policy should be established for handling data based on its classification. Appropriate personnel (e.g. data owner and compliance team) should review the data classification regularly.

8.2.4. *Data Transfer.* Data transfer guidelines should be established that provide clear guidance on security practices for data transfer. Measures should be in place to identify and remediate insecure data transfers.

8.2.5. *Data Protection Tools.* Data Loss Prevention solutions and similar tools should be considered to detect and block unauthorized transmission of sensitive data.

8.2.6. *Cryptography*. Well established international standards should be adopted when selecting encryption algorithm and encryption key length to protect sensitive data. Moreover, the authorized institution should regularly review and update its algorithms and/or increase the key lengths to ensure they remain resilient against evolving cyber threats.

8.2.7. *Data Disposal and Destruction.* Secure processes should be established for disposing of and destroying sensitive data. Sensitive data should be irrevocably deleted from devices, storage media or systems before such are being disposed.

8.3. Detection and Monitoring

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

8.3.2. *Logging.* An authorized institution should have a logging mechanism that provides good security monitoring and log protection. Logging should be implemented for security monitoring and detection of anomalous activities. Logging practices should be formally defined and documented, and regularly reviewed. These practices should include, but not limit to, log types for recording, retention periods, disposal methods, log masking requirements, and frequency of log collection and review.

8.3.3. *Monitoring*. A risk-based approach to monitoring should be adopted that covers multiple components (e.g. monitoring of high-risk networks, hosts, privileged access, file levels, etc.). Monitoring should take the form of automated alerts (e.g. emails, text messages) sent to designated response personnel for pre-defined events (e.g. high risk events with a low likelihood of false positives). These alerts should be properly monitored and reviewed. Security monitoring reports should be regularly sent to management and other personnel as required.

8.3.4. *Security Information and Event Management*. Processes and tools should be adopted for effective security monitoring. An authorized institution should consider adopting tools that consolidate logs from different sources (such as application logs, access logs, logs from network devices, sensitive data and intelligence feeds from third-party sources, and vulnerability assessment results) to perform correlation analysis and identify potential security threats. A user behavioural-based detection mechanism should be set up to detect malicious user or network activities, and emerging threats with predefined monitoring rules. Threat intelligence and indicators of compromise should also be taken into account when enhancing security monitoring. Detection capabilities should also be established for simultaneous attacks. Intelligence feeds should be regularly updated.

8.3.5. *Security Monitoring Team.* A qualified team (e.g. the Security Operation Centre team) should be dedicated to monitor security events. The roles and responsibilities of the security monitoring team members should be formally documented and clearly communicated.

8.4. Testing Programme and Methodologies

8.4.1. A testing programme should be established to validate the effectiveness of the authorized institution's technology and cyber risk management on a regular basis. The latest cyber threat intelligence should be employed when designing or updating the testing programme. When designing or updating the programme, key stakeholders (e.g. board and senior management and relevant business line management) and external stakeholders such as critical third-party should be involved. The conditions for triggering testing, and the frequency of testing should be identified.

The authorized institution should also establish a set of measures to avoid testing having any impact on its production systems. The testing programme should contribute to ongoing improvements to the institution's technology and cyber risk management.

8.4.2. *Vulnerability Assessment*. Vulnerability assessments should be regularly performed to identify and assess any system security vulnerabilities. The frequency of the vulnerability assessment should be commensurate with the criticality of the IT system and the security risk it is exposed to. Processes should be established to prioritize and remediate issues identified in vulnerability assessments, and to validate the remediation.

8.4.3. *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 frequency of the penetration testing should be commensurate with the criticality of the IT system and the security risk it is exposed to. The testing should be performed on the assets before they are placed into production and after major changes to the 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 penetration testing approach, other testing approaches such as black-box and grey-box style[7] 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.

8.4.4. *Threat Intelligence-Based Attack Simulation.* Authorized institutions should utilize threat intelligence analysis to create tailored, end-to-end cyber attack testing scenarios that are specific to both their own operations and the broader financial sector. These simulation tests should be carried out in a production environment to mimic real-life attack scenarios. Their purpose is to validate the effectiveness of existing security controls in protecting against real-world threats. Such simulation testing should be conducted in a controlled manner under close supervision to ensure that

[7] 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.

production systems are not impacted. If the potential impact on certain components within the production environment is deemed unacceptable, the authorized institution may consider conducting tests on a simulated component that closely resembles the production component. The simulation testing should be conducted in several phases, which include but are not limited to:

a) Scoping the critical functions mapped to key systems;
b) Leveraging threat intelligence to identify potential threat actors and the tactics, techniques, and procedures likely to be used in attacks on critical functions and target systems;
c) developing testing scenarios based on insights gained from threat intelligence;
d) conducting stealthy, intelligence-led tests against the critical functions and target systems; and
e) preparing relevant documentation to record the outcomes of the simulation testing.

The results of these tests should be reported to both the board and senior management, and effective risk mitigation controls should be applied to address any identified control gaps. The frequency of the simulation testing should be commensurate with the cyber risk profiles of the authorized institutions or should be performed upon notification from the AMCM.

8.4.5. *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.

8.5. *Remediation Management Process*. A formal remediation management process should be in place for handling vulnerabilities identified from the testing described in Section 8.4. A mechanism should also be set up to centrally track the remediation of vulnerabilities through their lifecycle. Ownership of vulnerability remediation should be assigned and properly recorded. All remediated vulnerabilities should be reassessed before they are treated as closed. The remediation status should be reported regularly to senior management.

8.6. *Qualified Testers*. All testing should be conducted by testers with adequate knowledge, experience and qualifications[8]. These testers should be

[8] Refer to Appendix A for an example of professional cybersecurity qualifications for intelligence-driven testing.

independent from the parties that design, implement or operate the controls, and should be able to report their findings freely and directly to the board and senior management.

9. RESPONSE AND RECOVERY

9.1. Business Continuity Planning [9]

9.1.1. *Business Continuity Management Programme.* A Business Continuity Management Programme should be set up, with a committee consisting of senior management and relevant stakeholders from business and IT having ownership of and responsibility for the programme. Roles and responsibilities should be fully established and endorsed by the committee. The Business Continuity Plan should be reviewed and updated at least annually. The Business Continuity Management Programme framework and policy should be operationalized across the authorized institution.

9.1.2. *Business Impact Analysis.* Business impact analysis, risk assessments and gap analysis should be conducted to keep the Business Continuity Management Programme up to date. A business impact analysis should be used to prioritize the recovery of services. A gap analysis should be conducted to identify any discrepancies between the Recovery Time Objective (RTO), the Recovery Point Objective (RPO), and the existing recovery capabilities. Key findings, and threats and vulnerabilities identified by the gap analysis should be reviewed and approved by the senior management.

9.1.3. *Crisis Management Plan.* A formal Crisis Management Plan should be developed for handling disruptive and unexpected cyber events, with clear roles and responsibilities assigned. Crisis escalation and incident management protocols should be established and consistently followed. The Crisis Management Plan should be reviewed and updated at least annually in line with emerging cyber threats.

9.1.4. *Disaster Recovery Plan.* A Disaster Recovery Plan should be established so that the authorized institution can recover its IT functions following a disaster. The plan should clearly document

[9] Refer also to the relevant requirements regarding Business Continuity Management (e.g. "Guideline on Business Continuity Management").

the recovery procedures and the capabilities required to recover information systems or technology components in different adverse scenarios. Testing is important for identifying improvements in the Disaster Recovery Plan and for familiarizing stakeholders with the plan. A disaster recovery drill should be integrated and functional in nature, in which business, IT and third-party service providers all participate. The Disaster Recovery Plan should be reviewed and updated at least annually, based on the drill results.

9.1.5. *Resources Management.* Teams responsible for business continuity and disaster recovery should be set up, trained and given clear roles. A budget should be planned and allocated at least annually, in alignment with the planned Business Continuity Management initiatives as approved by the respective committee.

9.2. Incident Management

9.2.1. *Incident Management Programme.* An incident management programme should be maintained, to provide visibility of incidents to the board and senior management, and to engage their ongoing oversight and support. The programme should cover areas such as incident identification, reporting, classification, handling, notification and recording.

9.2.2. *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 applied consistently throughout the incident triage process. Additional procedures for facilitating forensic investigations (e.g. digital evidence handling) should also be considered to support the incident response.

9.2.3. *Incident Classification Matrix.* An incident classification matrix should be established so that incidents can be clearly classified in order for the correct handling and reporting procedures to be applied. Different scenarios should be taken into consideration in the design of the incident classification matrix.

9.2.4. *Incident Communication and Reporting Requirements.* Incident communication and reporting requirements should cover both internal and external parties. External reporting requirements (such as those in response to regulatory or legal requirements) 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 they are accurately understood. Specific procedures should be defined and updated to ensure compliance and avoid errors or delays.

9.2.5. *Reporting to AMCM.* Incidents should be reported according to the requirements of "Incident Reporting Measures for Major Emergencies".

9.2.6. *Reporting to Cybersecurity Incident Alert and Response Centre (CARIC)* . In addition to reporting to AMCM, any technology and cyber security related incident should also be reported to CARIC according to the requirements of "Regulação de alerta, resposta e comunicação de incidentes da cibersegurança" (《網絡安全——事故預警、應對及通報規範》).

9.2.7. *Testing.* Regular testing of the authorized institution's incident response plan should take place. If significant change is made to the incident response plan, testing should be performed to ensure that the change does not affect business availability and the institution can still meet its business needs. The authorized institution should consider involving critical third parties in the testing. The results of the testing should be used to improve the incident response plan.

9.2.8. *Incident Management Team and Resources.* A cross-functional IR team should be assembled with the right skills and expertise to handle incidents falling within the scope of the incident management programme. The team should have relationships with functional authorities and industry groups that can be leveraged as needed. The board of the authorized institution should take final accountability for all incidents. Roles and responsibilities should be reviewed regularly, with capability gaps being identified and filled.

9.2.9. *Up-to-date Incident Management Programme.* The authorized institution's incident management programme should be kept up-to-date and responsive to emerging threats and technologies. Recent cases of cyber incidents and attacks could be used to continuously improve the programme and update the supporting components, such as testing scenarios and resource arrangements.

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

9.2.11. *Problem Management.* An authorized institution should establish a problem management process to ensure that it can determine and resolve the root causes of incidents, and take necessary measures to prevent their recurrence. Records of past incidents should include lessons learnt, to facilitate the diagnosis and resolution of future incidents with similar root causes. Additional analysis should be conducted on past incidents to verify that the root causes to the problems have been properly addressed.

10. **EMERGING TECHNOLOGY**

10.1. Emerging Technology Management Principle

10.1.1. *Emerging Technology Management Principle.* Many authorized institutions are adopting emerging technologies (e.g. Internet of Things (IoT), Artificial Intelligence (AI), and cloud computing technology [10]) to enhance their business and operational capabilities. However, the growing adoption of emerging technologies also introduces new risk management challenges. The board and senior management of an authorized institution should ensure that a proper governance framework and risk management measures are in place to oversee and manage the adoption of emerging technologies. The roles and responsibilities in managing the risks of emerging technologies should also be clearly defined in the governance framework.

10.2. Internet of Things

[10] Reference should also be made to the relevant requirements regarding the adoption of cloud computing technology (e.g. the "Guideline on Outsourcing" and the "Industry Guidance on Cloud Outsourcing Controls").

10.2.1. *Internet of Things.* The Internet of Things (IoT) refers to any electronic devices, including but not limited to multi-function printers, security cameras and smart televisions, that can be connected to the authorized institution's network or the Internet. The authorized institution should maintain an inventory of all its IoT devices. This should record both their locations on the network and their physical locations. As most IoT devices are designed with minimal security controls, it is important for authorized institutions to assess the function and criticality of the data that is collected, stored and processed by the IoT devices, and implement appropriate security measures. For instance, network access controls should be considered to restrict network traffic to and from IoT devices and prevent malware attacks. To further mitigate the IoT risks, authorized institutions should host IoT devices on a separate network segment from the network hosts the authorized institution's critical systems and sensitive data to reduce IoT risks. Moreover, authorized institutions should monitor their IoT devices for suspicious or anomalous system and network activities, and isolate the compromised devices if any malicious activity is detected.

10.3. Artificial Intelligence

10.3.1. *Governance of Artificial Intelligence.* A proper Artificial Intelligence governance framework, as well as technology and cyber risk management measures should be put in place to monitor the use of AI applications. Roles and responsibilities for monitoring the operations of AI applications should be defined in the framework. Before any AI application is adopted, its technology and cyber risk should be assessed by the authorized institution.

10.3.2. *Logging of AI applications*. As “black box” model is commonly adopted by AI during the computing process, an authorized institution should ensure that sufficient audit logs and other relevant documents are generated by AI applications to enable proper investigation in the case of unfavourable incidents or outcomes. The audit logs and documentation should be retained according to the relevant regulatory requirements.

10.3.3. *Data security of AI application*. Each AI application’s usage of sensitive data or personal identifiable information should be assessed. If sensitive or personal identifiable information is used,

data protection measures should be implemented in the AI application to protect such information in accordance with applicable local and overseas regulatory requirements.

10.3.4. *Cybersecurity measures*. As the adoption of AI applications may introduce new cybersecurity threats to an authorized institution, such as data poisoning and adversarial attacks, which exploit AI models through data manipulation. Authorized institution should review the AI computing process and the effectiveness of its security controls periodically to mitigate the risk with such threats.

10.3.5. *Contingency measures*. In addition to the security measures outlined above, an authorized institution should create a contingency plan that will promptly suspend the application if it generates unintended outcomes, and trigger fallback procedures.

10.4. Distributed Ledger Technology (DLT)

10.4.1. *Distributed Ledger Technology*. Distributed ledger (e.g., blockchain) technology refers to the protocols and infrastructure that allow computers in different locations to propose, validate, and record transactions in a synchronized manner across a network. Authorized institutions should thoroughly understand the use cases and identify and assess the potential risks and implications before adopting distributed ledger technology. Authorized institutions should also refer to the governance framework, international standards, guidelines, circulars and white papers developed by other regulatory authorities in order to stay updated on best practices for managing the specific risks associated with this technology.

11. **INDEPENDENT ASSESSMENT**

11.1. Independent Assessment of Technology and Cyber Risk Management

11.1.1. *Independent Assessment.* An independent assessment of an authorized institution's technology and cyber risk management (which should, at a minimum, cover paragraphs 4 to 10 of this Guideline) should be performed at least every two years or upon notification from AMCM. Those performing the independent assessment should have, and be able to demonstrate, the necessary

expertise[11] in the relevant fields. They should be independent from the parties that develop or administer the system, and not involved in the operations to be reviewed or in selecting or implementing the relevant control measures to be reviewed. They should be able to report findings freely and directly to the authorized institution's board and senior management. If meeting the above criteria, the assessors can be internal staff (e.g. internal auditors) or an external party (e.g. an external auditor or another third-party service provider). The results should be approved by senior management and the report should be submitted to AMCM. It should include at least the following items:

a) time of assessment;
b) scope and approach adopted;
c) the assessors' findings and recommendations; and
d) management responses.

11.2. Reference to Industry Standards and Practices

11.2.1. An authorized institution should consider referring to different industry standards and practices to provide itself with a benchmark for evaluating and enhancing its technology and cyber risk management controls.

12. **SUPERVISORY APPROACH**

12.1. The AMCM expects each authorized institution to develop and implement effective technology and cyber risk management systems that are consistent with the above-mentioned principles and key processes.

12.2. While this guideline does not dictate specific means or technologies, the AMCM expects each authorized institution to implement relevant controls or demonstrate effective means to fulfil such controls in accordance with its technology and cyber risk profile. An authorized institution should consider the following areas when evaluating its risk profile:

a) Technologies and connection types

[11] Refer to Appendix A for an example of the professional qualifications required for conducting an independent assessment of technology and cyber risk management.

b) Delivery channels
c) Online / mobile products and technology services
d) Organizational characteristics
e) Internal and external threats

12.3. If an authorized institution is a branch of an overseas incorporated bank relying on its head / regional office to execute the roles and responsibilities of technology and cyber risk management, it is still expected to demonstrate that such approach fulfils the requirements, and does not undermine the authorized institution's technology and cyber risk management. The authorized institution should note that, depending on the circumstances, its governance responsibilities may still need to be executed by local branch management.

12.4. Prior to launching relevant services, or adopting emerging technologies, or undertaking major enhancements to its existing systems or services, an authorized institution is expected to have in place adequate technology and cyber risk management practices in accordance with this Guideline, or have completed relevant remediation of any major non-compliance / cybersecurity incidents.

12.5. The AMCM will, in the course of its onsite examinations and offsite reviews, determine as appropriate the adequacy of an authorized institution's technology and cyber risk management practices based on the requirements set out in this Guideline. Authorized institution is expected to comply with this Guideline as soon as practicable and within 12 months of the date of this Guideline.

APPENDIX A: REFERENCES FOR PROFESSIONAL QUALIFICATIONS

Qualifications for Independent Assessment of Technology and Cyber Risk 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).
- ISC² Certified Information Systems Security Professional (CISSP)
- EC-Council Certified Ethical Hacker (CEH)

Qualifications for Penetration Testing / Threat Intelligence-Based Attack Simulation

- 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)
- Altered Security's Certified Red Teaming Expert (CRTE)
- Altered Security's Certified Red Teaming Professional (CRTP)
- eLearnSecurity Certified Penetration Tester (eCPTX)
- eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX)

Threat Intelligence Specialist Qualifications

- CREST Certified Threat Intelligence Manager (CCTIM)
- CREST Registered Threat Intelligence Analyst (CRTIA)
- GIAC Cyber Threat Intelligence (GCTI)
- GIAC Penetration Tester (GPEN)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- HKIB's CCASP - Certified Simulated Attack Manager
- McAfee Institute's Certified Cyber Intelligence Professional (CCIP)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Exploitation Expert (OSEE)

APPENDIX B: REFERENCES FOR 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