Technology Risk Management Guidelines

January 2021

Monetary Authority of Singapore

Contents

1 Preface

1.1 The technology landscape of the financial sector is transforming at a rapid pace and the underlying information technology (IT) infrastructure supporting financial services has grown in scope and complexity in recent years. Many financial institutions (FIs) are riding the wave of digitalisation to increase operational efficiency and to deliver better services to consumers.

1.2 Digital transformation in the financial sector can be broadly characterised by the adoption of new technology and the use of existing technology in innovative ways to achieve greater automation and enrich financial service offerings.

1.3 While digital transformation brings significant benefits to the financial ecosystem, it also increases FIs' exposure to a range of technology risks, including cyber risk. The techniques used by cyber threat actors are becoming increasingly sophisticated, and weak links in the interconnected financial ecosystem can be compromised to carry out fraudulent financial transactions, exfiltrate sensitive financial data or disrupt IT systems that support financial services. Hence, each FI should seek to understand their exposure to technology risks and put in place a robust risk management framework to ensure IT and cyber resilience.

1.4 The revised MAS Technology Risk Management Guidelines set out technology risk management principles and best practices for the financial sector, to guide FIs in the following:

(a) Establish Sound and Robust Technology Risk Governance and Oversight

The board of directors and senior management at an FI play an integral part in the oversight and management of technology risk. The board of directors and senior management should cultivate a strong risk culture, and ensure the establishment of a sound and robust technology risk management framework.

(b) Maintain Cyber Resilience

Strong cyber resilience is critical for sustaining trust and confidence in financial services. FIs should adopt a defence-in-depth approach to strengthening cyber resilience. It is also important that FIs establish and continuously improve their IT processes and controls to preserve confidentiality, integrity and availability of data and IT systems.

2 Application of the MAS Technology Risk Management Guidelines

2.1 The aim of the MAS Technology Risk Management Guidelines (hereafter referred as "the Guidelines") is to promote the adoption of sound and robust practices for the management of technology risk.

2.2 The Guidelines do not affect, and should not be regarded as a statement of the standard of care owed by FIs to their customers. The extent and degree to which an FI implements the Guidelines should be commensurate with the level of risk and complexity of the financial services offered and the technologies supporting such services. In supervising an FI, the degree of observance with the spirit of the Guidelines by an FI is an area of consideration by MAS.

2.3 These Guidelines provide general guidance, and are not intended to be comprehensive nor replace or override any legislative provisions. They should be read in conjunction with the provisions of the relevant legislation, the subsidiary legislation made under the relevant legislation, as well as written directions, notices, codes and other guidelines that MAS may issue from time to time pursuant to the relevant legislation and subsidiary legislation.

3 Technology Risk Governance and Oversight

3.1 Role of the Board of Directors and Senior Management

3.1.1 Technology is a key business enabler in the financial sector and FIs rely on technology to deliver financial services. It is vital that the FI's board of directors and senior management ensure effective internal controls and risk management practices are implemented to achieve security, reliability and resilience of its IT operating environment.

3.1.2 Both the board of directors and senior management should have members with the knowledge to understand and manage technology risks, which include risks posed by cyber threats.

3.1.3 The board of directors and senior management should ensure a Chief Information Officer, Chief Technology Officer or Head of IT, and a Chief Information Security Officer or Head of Information Security[1], with the requisite expertise and experience, are appointed. The appointments should be minimally approved by the Chief Executive Officer.

3.1.4 The board of directors and senior management should ensure a technology risk management strategy is established and implemented.

3.1.5 The board of directors and senior management should ensure key IT decisions are made in accordance with the FI's risk appetite.

3.1.6 Given that technology underpins many of the operations and services offered by an FI, the board of directors and senior management should set the tone from the top and cultivate a strong culture of technology risk awareness and management at all levels of staff within the FI.

---

[1] *"chief information officer", "chief technology officer",* or *"head of information technology"*, who is principally responsible for establishing and implementing the overall information technology strategy, overseeing the day-to-day information technology operations, and managing the information technology risks of the financial institution.
"chief information security officer" or *"head of information security"*, who is principally responsible for the information security strategy and programme of the financial institution, including but not limited to information security policies and procedures to safeguard information assets, information security controls, and the management of information security.

- *Guidelines on Individual Accountability and Conduct, Annex B*

3.1.7 The board of directors or a committee delegated by it, is responsible for:

(a) ensuring a sound and robust risk management framework is established and maintained to manage technology risks;

(b) ensuring there is a technology risk management function to oversee the technology risk management framework and strategy, as well as to provide an independent view of the technology risks faced by the FI;

(c) giving senior executives, who are responsible for executing the FI's technology risk management strategy, sufficient authority, resources and access to the board of directors;

(d) approving the risk appetite and risk tolerance statement that articulates the nature and extent of technology risks that the FI is willing and able to assume;

(e) undertaking regular reviews of the technology risk management strategy for continued relevance;

(f) assessing management competencies for managing technology risks; and

(g) ensuring an independent audit function is established to assess the effectiveness of controls, risk management and governance of the FI.

3.1.8 Senior management is responsible for:

(a) establishing the technology risk management framework and strategy;

(b) managing technology risks based on the established framework and strategy;

(c) ensuring sound and prudent policies, standards and procedures for managing technology risks are established and maintained, and that standards and procedures are implemented effectively;

(d) ensuring the roles and responsibilities[2] of staff in managing technology risks are delineated clearly; and

(e) apprising the board of directors of salient and adverse technology risk developments and incidents that are likely to have a major impact on the FI in a timely manner.

3.2 Policies, Standards and Procedures

3.2.1 The FI should establish policies, standards and procedures and, where appropriate, incorporate industry standards and best practices to manage technology risks and safeguard information assets[3] in the FI. The policies, standards and procedures should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape.

3.2.2 The FI should ensure risks associated with deviations are thoroughly reviewed and assessed. The risk assessment should be approved by senior management. Approved deviations should be reviewed periodically to ensure the residual risks remain at an acceptable level.

3.2.3 Compliance processes should be implemented to verify that policies, standards and procedures are adhered to. These include follow-up processes for non-compliance.

3.3 Management of Information Assets

3.3.1 To have an accurate and complete view of its IT operating environment, the FI should establish information asset management practices that include the following:

(a) identification of information assets that support the FI's business and delivery of financial services;

[2] The roles and responsibilities of senior management and staff could be defined and tracked using a Responsibility Assignment Matrix, also known as RACI. The RACI matrix outlines who are responsible and accountable for the functions, as well as who should be consulted or informed.

[3] Information assets include data, hardware and software. Information assets are not limited to those that are owned by the FI. They also include those that are entrusted to the FI by customers or third parties, rented or leased by the FI, and those that are used by service providers to deliver their services to the FI. Adapted from CPMI-IOSCO, *Guidance on Cyber Resilience for Financial Market* Infrastructures, June 2016.

(b) classification of an information asset based on its security classification or criticality;

(c) ownership of information assets, and the roles and responsibilities of the staff managing the information assets; and

(d) establishment of policies, standards and procedures to manage information assets according to their security classification or criticality.

3.3.2 The FI should maintain an inventory of all its information assets. The inventory should be reviewed periodically and updated whenever there are changes.

3.4 Management of Third Party Services

3.4.1 The use of certain third party services by FIs may not always constitute outsourcing. However, as many of these services are provisioned or delivered using IT, or may involve confidential or sensitive customer information being stored or processed electronically by the third party, the FI's operations and its customers may be adversely impacted if there is a system failure or security breach at the third party.

3.4.2 The FI should assess and manage its exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third party before entering into a contractual agreement or partnership.

3.4.3 On an ongoing basis, the FI should ensure the third party employs a high standard of care and diligence in protecting data confidentiality[4] and integrity as well as ensuring system resilience.

3.5 Competency and Background Review

3.5.1 As the human element plays an important role in managing IT systems and processes in an IT environment, the FI should ensure personnel, including contractors and service providers, have the requisite level of competence and skills to perform the IT functions and manage technology risks.

[4] Data confidentiality refers to the protection of sensitive or confidential data such as customer details from unauthorised access and disclosure.

3.5.2 Insider threat, which includes theft of confidential data, sabotage of IT systems and fraud by staff, contractors and service providers, is considered one of the risks to an organisation. A background check on personnel, who has access to the FI's data and IT systems, should be performed to minimise this risk.

3.6 Security Awareness and Training

3.6.1 A comprehensive IT security awareness training programme should be established to maintain a high level of awareness among all staff in the FI. The content of the training programme should minimally include information on the prevailing cyber threat landscape and its implications, the FI's IT security policies and standards, as well as an individual's responsibility to safeguard information assets. All personnel in the FI should be made aware of the applicable laws, regulations, and guidelines pertaining to the use of, and access to, information assets.

3.6.2 The training programme should be conducted at least annually for all staff, contractors and service providers who have access to the FI's information assets.

3.6.3 The board of directors should undergo training to raise their awareness on risks associated with the use of technology and enhance their understanding of technology risk management practices.

3.6.4 The training programme should be reviewed periodically to ensure its contents remain current and relevant. The review should take into consideration changes in the FI's IT security policies, prevalent and emerging risks, and the evolving cyber threat landscape.

4 Technology Risk Management Framework

4.1 Risk Management Framework

4.1.1 The FI should establish a risk management framework to manage technology risks. Appropriate governance structures and processes should be established, with well-defined roles, responsibilities, and clear reporting lines across the various organisational functions.

4.1.2 Effective risk management practices and internal controls should be instituted to achieve data confidentiality and integrity, system security and reliability, as well as stability and resilience in its IT operating environment.

4.1.3 The risk owner, who is accountable for ensuring proper risk treatment measures are implemented and enforced for a specific technology risk, should be identified. The role of the risk owner may be assumed by a function or group of functions within the FI, who is given the authority to manage technology risks.

4.1.4 The framework should also encompass the following components:

(a) risk identification – identify threats and vulnerabilities to the FI and information assets;

(b) risk assessment – assess the potential impact and likelihood of threats and vulnerabilities to the FI and information assets;

(c) risk treatment – implement processes and controls to manage technology risks posed to the FI and protect the confidentiality, integrity and availability of information assets; and

(d) risk monitoring, review and reporting – monitor and review technology risks, which include risks that customers are exposed to, changes in business strategy, IT systems, environmental or operating conditions; and report key risks to the board of directors and senior management.

4.1.5 As business and IT environments, as well as the cyber threat landscape, tend to evolve over time, the FI should review the adequacy and effectiveness of its risk management framework regularly.

4.2 Risk Identification

4.2.1 The FI should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the FI and its stakeholders include internal sabotage, malware and data theft.

4.3 Risk Assessment

4.3.1 The FI should perform an analysis of the potential impact and consequences of the threats and vulnerabilities on the overall business and operations. The FI should take into consideration financial, operational, legal, reputational and regulatory factors in assessing technology risks.

4.3.2 To facilitate the prioritisation of technology risks, a set of criteria measuring and determining the likelihood and impact of the risk scenarios should be established.

4.4 Risk Treatment

4.4.1 The FI should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance. The IT control and risk mitigation approach should be subject to regular review and update, taking into account the changing threat landscape and variations in the FI's risk profile.

4.4.2 As there are residual risks from threats and vulnerabilities which cannot be fully eliminated, the FI should assess whether risks have been reduced to an acceptable level after applying the mitigating measures. The criteria and approving authorities for risk acceptance should be clearly defined and it should be commensurate with the FI's risk tolerance.

4.4.3 The FI should take insurance cover for various insurable technology risks to reduce financial impact such as recovery and restitution costs.

4.5 Risk Monitoring, Review and Reporting

4.5.1 The FI should institute a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks.

4.5.2 A risk register should be maintained to facilitate the monitoring and reporting of technology risks. Significant risks should be monitored closely and reported to the board of directors and senior management. The frequency of monitoring and reporting should be commensurate with the level of risk.

4.5.3 To facilitate risk reporting to management, technology risk metrics should be developed to highlight information assets that have the highest risk exposure. In determining the technology risk metrics, the FI should take into account risk events and audit observations, as well as applicable regulatory requirements.

5 IT Project Management and Security-by-Design

5.1 Project Management Framework

5.1.1 A project management framework should be established to ensure consistency in project management practices, and delivery of outcomes that meets project objectives and requirements. The framework should cover the policies, standards, procedures, processes and activities to manage projects from initiation to closure.

5.1.2 Detailed IT project plans should be established for all IT projects. An IT project plan should set out the scope of the project, as well as the activities, milestones and the deliverables to be realised at each phase of the project. The roles and responsibilities of staff involved in the project should be clearly defined in the plan.

5.1.3 Key documentation in the IT project life cycle, including the feasibility analysis, cost-benefit analysis, business case analysis, project plan, as well as the implementation plan, should be maintained and approved by the relevant business and IT management.

5.1.4 As project risks can adversely impact the IT project delivery timeline, budget and quality of the project deliverables, a risk management process should be established to identify, assess, treat and monitor the attendant risks throughout the project life cycle.

5.2 Project Steering Committee

5.2.1 For large and complex projects that impact the business, a project steering committee consisting of key stakeholders, including business owners and IT, should be formed to provide direction, guidance and oversight to ensure milestones are reached, and deliverables are realised in a timely manner.

5.2.2 Risks and issues for large and complex projects, which cannot be resolved at the project management level, should be escalated to the project steering committee and senior management.

5.3 System Acquisition

5.3.1 The FI should establish standards and procedures for vendor evaluation and selection to ensure the selected vendor is qualified and able to meet its project requirements and deliverables. The level of assessment and due diligence performed should be commensurate with the criticality of the project deliverables to the FI.

5.3.2 It is important that the FI assesses the robustness of the vendor's software development and quality assurance practices, and ensures stringent security practices are in place to safeguard and protect any sensitive data the vendor has access to over the course of the project. Any vendor access to the FI's IT systems should be controlled and monitored.

5.3.3 If a project involves a commercial off-the-shelf (COTS) solution that does not meet the FI's security requirements, the FI should assess the risks and ensure adequate mitigating controls are implemented to address the risks before the solution is deployed.

5.3.4 The FI should assess if a source code escrow agreement should be in place, based on the criticality of the acquired software to the FI's business, so that the FI can have access to the source code in the event that the vendor is unable to support the FI. Suitable alternatives to replace the software should be identified if an escrow agreement could not be implemented.

5.4 System Development Life Cycle and Security-By-Design

5.4.1 The FI should establish a framework to manage its system development life cycle (SDLC). [5] The framework[6] should clearly define the processes, procedures and controls in each phase of the life cycle, such as initiation/planning, requirements analysis, design, implementation, testing and acceptance. Standards and procedures for the different phases of the SDLC should be maintained.

5.4.2 The security-by-design approach refers to building security in every phase of the SDLC in order to minimise system vulnerabilities and reduce the attack surface. The FI should incorporate security specifications in the system design, perform continuous security evaluation, and adhere to security practices throughout the SDLC.

5.4.3 Security requirements should minimally cover key control areas such as access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling.

[5] The overall process of developing/acquiring and managing systems from initiation/planning, requirements gathering, design, implementation, testing, deployment and maintenance to disposal.

[6] Within the SDLC framework, it includes models or methodologies such as Waterfall and Agile.

5.4.4 The SDLC should, where relevant, involve the IT security function in each phase of the life cycle.

5.5 System Requirements Analysis

5.5.1 The FI should identify, define and document the functional requirements for the IT system. In addition to functional requirements, key requirements such as system performance, resilience and security controls, should also be established and documented.

5.5.2 In establishing the security requirements, the FI should assess the potential threats and risks related to the IT system, and determine the acceptable level of security required to meet its business needs.

5.6 System Design and Implementation

5.6.1 As part of the design phase, the FI should review the proposed architecture and design of the IT system, including the IT controls to be built into the system, to ensure they meet the defined requirements, before implementation.

5.6.2 The FI should verify that system requirements are met by the current system design and implementation. Any changes to, or deviations from, the defined requirements should be endorsed by relevant stakeholders.

5.6.3 Relevant domain experts should be engaged to participate in the design review. For example, the security design and architecture of the IT system should be reviewed by IT security specialists or qualified security consultants.

5.7 System Testing and Acceptance

5.7.1 A methodology for system testing[7] should be established. The scope of testing should cover business logic, system function, security controls and system performance under various load and stress conditions. A test plan should be established and approved before testing.

[7] System testing includes unit, modular, integration, system and user acceptance testing.

5.7.2 The FI should trace the requirements during the testing phase, and ensure each requirement is covered by appropriate test cases.

5.7.3 The FI should maintain separate physical or logical environments for unit, system integration and user acceptance testing, and restrict access to each environment on a need-to basis.

5.7.4 The FI should perform regression testing for changes (e.g. enhancement, rectification, etc.) to an existing IT system to validate that it continues to function properly after the changes have been implemented.

5.7.5 Issues identified from testing, including system defects or software bugs, should be properly tracked and addressed. Major issues that could have an adverse impact on the FI's operations or delivery of service to customers should be reported to the project steering committee and addressed prior to deployment to the production environment.

5.7.6 The FI should ensure the results of all testing that was conducted are documented in the test report, and signed off by the relevant stakeholders.

5.8 Quality Management

5.8.1 During project planning, the FI should define the expected quality attributes and the assessment metrics for the project deliverables based on its quality control standards.

5.8.2 Quality assurance should be performed by an independent quality assurance function to ensure project activities and deliverables comply with the FI's policies, procedures and standards.

6 Software Application Development and Management

6.1 Secure Coding, Source Code Review and Application Security Testing

6.1.1 Software bugs or vulnerabilities are typically targeted and exploited by threat actors to compromise an IT system, and they often occur because of poor software development practices. To minimise the bugs and vulnerabilities in its software, the FI should adopt standards on secure coding, source code review[8] and application security testing.

6.1.2 The secure coding and source code review standards should cover areas such as secure programming practices, input validation, output encoding, access controls, authentication, cryptographic practices, and error and exception handling.

6.1.3 A policy and procedure on the use of third party and open-source software codes should be established to ensure these codes are subject to review and testing before they are integrated into the FI's software.

6.1.4 To facilitate the remediation of vulnerabilities in a timely manner, the FI should keep track of updates and reported vulnerabilities for third party and open-source software codes that are incorporated in the FI's software.

6.1.5 The FI should ensure its software developers are trained or have the necessary knowledge and skills to apply the secure coding and application security standards when developing applications.

6.1.6 It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current.

[8] Source code review is a systematic and methodical examination of the source code of an application, with the objective of finding coding errors, poor coding practices or other software defects.

6.1.7 All issues and software defects discovered from the source code review and application security testing should be tracked. Major issues and software defects should be remediated before production deployment.

6.2 Agile Software Development

6.2.1 Agile software development is based on an iterative and incremental development model to accelerate software development and delivery to respond to business and customer needs. When adopting Agile software development methods, the FI should continue to incorporate the necessary SDLC and security-by-design principles throughout its Agile process.

6.2.2 The FI should ensure secure coding, source code review and application security testing standards are applied during Agile software development.

6.3 DevSecOps Management

6.3.1 DevSecOps is the practice of automating and integrating IT operations, quality assurance and security practices in the software development process. It constitutes continuous integration, continuous delivery and IT security practices for frequent, efficient, reliable and secure development, testing and release of software products. The FI should ensure its DevSecOps activities and processes are aligned with its SDLC framework and IT service management processes (e.g. configuration management, change management, software release management).

6.3.2 The FI should implement adequate security measures and enforce segregation of duties for the software development, testing and release functions in its DevSecOps processes.

6.4 Application Programming Interface Development

6.4.1 Application programming interfaces (APIs)[9] enable various software applications to communicate and interact with each other and exchange data. Open APIs are publicly available APIs that provide developers with programmatic access to a software application or web service. FIs may collaborate with FinTech companies and develop open APIs, which

[9] APIs are sets of protocols that define how one application interacts with another, usually to facilitate an information exchange.

are used by third parties to implement products and services for customers and the marketplace. Hence, it is important for the FI to establish adequate safeguards to manage the development and provisioning of APIs for secure delivery of such services.

6.4.2 A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the FI via APIs, as well as governing third party API access. The vetting criteria should take into account factors such as the third party's nature of business, cyber security posture, industry reputation and track record.

6.4.3 The FI should perform a risk assessment before allowing third parties to connect to its IT systems via APIs, and ensure the implementation for each API is commensurate with the sensitivity and business criticality of the data being exchanged, and the confidentiality and integrity requirements of the data.

6.4.4 Security standards for designing and developing secure APIs should be established. The standards should include the measures to protect the API keys or access tokens,[10] which are used to authorise access to APIs to exchange confidential data. A reasonable timeframe should be defined and enforced for access token expiry to reduce the risk of unauthorised access.

6.4.5 Strong encryption standards and key management controls should be adopted to secure transmission of sensitive data through APIs.

6.4.6 A robust security screening and testing of the API should be performed between the FI and its third parties before it is deployed into production. The FI should log the access sessions by third parties, such as the identity of the party making the API connections, date and time, as well as the data being accessed.

6.4.7 Detective measures, such as technologies that provide real-time monitoring and alerting, should be instituted to provide visibility of the usage and performance of APIs, and detect suspicious activities. Robust measures should be established to promptly revoke the API keys or access token in the event of a breach.

[10] An access token contains credentials that are used to validate the requestor and ensure the requestor has the permissions to access the requested data or perform the requested operations.

6.4.8 The FI should ensure adequate system capacity is in place to handle high volumes of API call requests, and implement measures to mitigate cyber threats such as denial of service (DoS) attacks.

6.5 Management of End User Computing and Applications

6.5.1 The prevalence of business application tools and software on the Internet has enabled end user computing, where business users develop or use simple applications to automate their operations, such as performing data analysis and generating reports. IT hardware, software and services that are not managed by the IT department (shadow IT) increase the FI's exposure to risks such as leakage of sensitive data or malware infection. Shadow IT should be managed as part of the FI's information assets.

6.5.2 The FI should establish measures to control and monitor the use of shadow IT in its environment.

6.5.3 A process should be established to assess the risk of end user developed or acquired applications to the FI, and ensure appropriate controls and security measures are implemented to address the identified risks, and approval is obtained before being used. The FI should ensure proper testing before the applications are deployed.

7 IT Service Management

7.1 IT Service Management Framework

7.1.1 A robust IT service management framework is essential for supporting IT services and operations, tracking information assets, managing changes, responding to incidents, as well as ensuring the stability of the production IT environment. The framework should comprise the governance structure, processes and procedures for IT service management activities including configuration management, technology refresh management, patch management, change management, software release management, incident management and problem management.

7.2 Configuration Management

7.2.1 Configuration management is the process of maintaining key information (e.g. model, version, specifications, etc.) about the configuration of the hardware and software that makes up each IT system. The FI should implement a configuration management process to maintain accurate information of its hardware and software to have visibility and effective control of its IT systems.

7.2.2 The FI should review and verify the configuration information of its hardware and software on a regular basis to ensure it is accurate and up-to-date.

7.3 Technology Refresh Management

7.3.1 The FI should avoid using outdated and unsupported hardware or software, which could increase its exposure to security and stability risks. The FI should closely monitor the hardware's or software's end-of-support (EOS) dates as service providers would typically cease the provision of patches, including those relating to security vulnerabilities that are found after the EOS date.

7.3.2 A technology refresh plan for the replacement of hardware and software should be developed before they reach EOS. A risk assessment for hardware and software approaching EOS date should be conducted to evaluate the risks of their continued use, and effective risk mitigation measures should be implemented.

7.3.3 The FI should obtain dispensation from its management for the continued use of outdated and unsupported hardware and software. The dispensation should be assigned a validity period that is commensurate with the identified risks and risk mitigation measures. The dispensation should be reviewed periodically to ensure the attendant risks remain at an acceptable level.

7.4 Patch Management

7.4.1 A patch management process should be established to ensure applicable functional and non-functional patches (e.g. fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with the criticality of the patches and the FI's IT systems.

7.4.2 Patches should be tested before they are applied to the FI's IT systems in the production environment to ensure compatibility with existing IT systems or they do not introduce problems to the IT environment.

7.5 Change Management

7.5.1 The FI should establish a change management process to ensure changes to information assets are assessed, tested, reviewed and approved before implementation.

7.5.2 A risk and impact analysis of the change to an information asset should be conducted before implementing the change. The analysis should cover factors such as security and implications of the change in relation to other information assets.

7.5.3 The FI should ensure all changes are adequately tested in the test environment. Test plans for changes should be developed and approved by the relevant business and IT management. Test results should be accepted and signed off before the changes are deployed to the production environment.

7.5.4 A change advisory board, comprising key stakeholders including business and IT management, should be formed to approve and prioritise the changes after considering the stability and security implications of the changes to the production environment.

7.5.5 The FI should perform a backup of the information asset prior to the change implementation, and establish a rollback plan to revert the information asset to the previous state if a problem arises during or after the change implementation.

7.5.6 Urgent or emergency changes, such as a high priority security patch for an IT system, are changes that need to be implemented expeditiously and may not be able to follow the standard change management process. To reduce the risk to the security and stability of the production environment, the FI should clearly define the procedures for assessing, approving and implementing emergency changes, as well as identify the authorisers or approvers for the changes.

7.5.7 Logs contain useful information which facilitates investigations and troubleshooting. As such, the FI should ensure the logging facility is enabled to record activities that are performed during the change process.

7.6 Software Release Management

7.6.1 Segregation of duties in the software release process should be practised to ensure no single individual has the ability to develop, compile and move software codes[11] from one environment to another.

7.6.2 It is important that controls are implemented to maintain traceability and integrity for all software codes that are moved between IT environments.

7.7 Incident Management

7.7.1 An IT incident occurs when there is an unexpected disruption to the delivery of IT services or a security breach of an IT system, which compromises the confidentiality, integrity and availability of data or the IT system. The FI should establish an incident management framework with the objective of restoring an affected IT service or system to a secure and stable state, as quickly as possible, so as to minimise impact to the FI's business and customers.

7.7.2 The FI should ensure sufficient resources are available to facilitate and support incident response and recovery. The FI may engage external assistance to augment its resources to facilitate and support incident response and recovery. For example, the FI can engage an incident response and security forensic company to support cyber attack investigation, and provide 24 by 7 incident response capability.

[11] Source codes, byte codes and binaries

7.7.3 The incident management framework should minimally cover:

(a) the process and procedure for handling IT incidents, including cyber related incidents;[12]

(b) maintenance and protection of supporting evidence for the investigation and diagnosis of incidents; and

(c) the roles and responsibilities of staff and external parties involved in recording, analysis, escalation, decision-making, resolution and monitoring of incidents.

7.7.4 The FI should configure system events or alerts to provide an early indication of issues that may affect its IT systems' performance and security. System events or alerts should be actively monitored so that prompt measures can be taken to address the issues early.

7.7.5 In some situations, a major incident may develop unfavourably into a crisis. The FI should regularly apprise its senior management of the status of major incidents so that decisions to mitigate the impact of the crisis can be made in a timely manner, such as activation of IT disaster recovery.

7.7.6 A communications plan that covers the process and procedures to apprise customers of impact on services, and to handle media or public queries should be maintained. The plan should also include identifying the spokespersons and subject matter experts to address the media or public queries as well as the communication channels to disseminate information.

7.7.7 It would be useful for the FI to provide timely updates to its customers on the progress of its incident management and the measures the FI is implementing to protect its customers and continue delivery of financial services. Where appropriate, the FI should advise its customers on actions that they should take to protect themselves.

[12] Examples of cyber incidents include malware infection, social engineering, man-in-the-middle attack, denial of service attack, etc.

7.8 Problem Management

7.8.1 The FI should establish problem management process and procedures to determine and resolve the root cause of incidents to prevent the recurrence of similar incidents.

7.8.2 The FI should maintain a record of past incidents which include lessons learnt to facilitate the diagnosis and resolution of future incidents with similar characteristics.

7.8.3 A trend analysis of past incidents should be performed by the FI to identify commonalities and patterns in the incidents, and verify if the root causes to the problems had been properly identified and resolved. The FI should also use the analysis to determine if further corrective or preventive measures are necessary.

8 IT Resilience

8.1 System Availability

8.1.1 Maintaining system availability is crucial in achieving confidence and trust in the FI's operational capabilities. IT systems should be designed and implemented to achieve the level of system availability that is commensurate with its business needs.

8.1.2 Redundancy or fault-tolerant solutions should be implemented for IT systems which require high system availability. The FI should perform a periodic review of its IT system and network architecture design to identify weaknesses in the existing design. The review should include a mapping of internal and external dependencies of the FI's IT systems to determine any single point of failure. It is important that the FI conducts regular testing to ascertain that the level of resilience continues to meet its business requirements.

8.1.3 The FI should continuously monitor the utilisation of its system resources against a set of pre-defined thresholds.[13] Such monitoring could facilitate the FI in carrying out capacity management to ensure IT resources are adequate to meet current and future business needs.

8.1.4 Procedures should be established to respond to situations when pre-defined thresholds for system resources and system performance have been breached.

8.2 System Recoverability

8.2.1 The FI should establish systems' recovery time objectives (RTO) and recovery point objectives (RPO) that are aligned to its business resumption and system recovery priorities.

8.2.2 The FI's disaster recovery plan should include procedures to recover systems from various disaster scenarios, as well as the roles and responsibilities of relevant personnel in the recovery process. The disaster recovery plan should be reviewed at least

[13] The monitoring of system resources could cover the utilisation of the computing processor, memory and data storage. For network resources, the monitoring indicators could cover network throughput, latency and packet loss.

annually and updated when there are material changes to business operations, information assets or environmental factors.

8.2.3 During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management. The FI should avoid deviating from the plan as untested recovery measures could exacerbate the incident and prolong the recovery process. In exceptional circumstances where untested recovery measures need to be used, the FI should perform a risk assessment and ensure adequate controls are in place, as well as obtain approval from senior management.

8.2.4 The FI should endeavour to operate from its recovery, secondary or alternate site periodically so as to have the assurance that its infrastructure and systems at these sites are able to support business needs for an extended period of time when production systems failover from the primary or production site.

8.3 Testing of Disaster Recovery Plan

8.3.1 The FI should perform regular testing of its disaster recovery plan to validate the effectiveness of the plan and ensure its systems are able to meet the defined recovery objectives. Relevant stakeholders, including those in business and IT functions, should participate in the disaster recovery test to familiarise themselves with the recovery processes and ascertain if the systems are performing as expected.

8.3.2 A disaster recovery test plan should include the test objectives and scope, test scenarios, test scripts with details of the activities to be performed during and after testing, system recovery procedures, and the criteria for measuring the success of the test.

8.3.3 The testing of disaster recovery plan should comprise:

(a) various plausible disruption scenarios, including full and partial incapacitation of the primary or production site and major system failures; and

(b) recovery dependencies between information assets, including those managed by third parties.

8.3.4 Where information assets are managed by service providers, the FI should assess the service provider's disaster recovery capability and ensure disaster recovery arrangements for these information assets are established, tested and verified to meet its

business needs. The FI should engage its service provider to test the recovery steps that require coordinated actions between the service provider and the FI.

8.4 System Backup and Recovery

8.4.1 The FI should establish a system and data backup strategy, and develop a plan to perform regular backups so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted.

8.4.2 To ensure data availability is aligned with the FI's business requirements, the FI should institute a policy to manage the backup data life cycle, which includes the establishment of the frequency of data backup and data retention period, management of data storage mechanisms, and secure destruction of backup data.

8.4.3 The FI should periodically test the restoration of its system and data backups to validate the effectiveness of its backup restoration procedures.

8.4.4 To protect data in backup from unauthorised access and modification, the FI should ensure any confidential data stored in the backup media is secured (e.g. encrypted). Backup media should be stored offline or at an offsite location.

8.5 Data Centre Resilience

8.5.1 The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centres (DCs) to identify potential vulnerabilities and weaknesses, and the protection that should be established to safeguard the DCs against physical and environmental threats.[14] In addition, the TVRA should consider the political and economic climate of the country in which the DCs are located. The TVRA should be reviewed whenever there is a significant change in the threat landscape or when there is a material change in the DC's environment.

8.5.2 The FI should ensure adequate redundancy for the power, network connectivity, and cooling, electrical and mechanical systems of the DC to eliminate any single point of failure. Consideration should be given to the following:

[14] Examples: flooding, fire, natural disasters, acts of terrorism, electricity surge, electromagnetic and electrical interference, etc.

(a) diversification of data communications and network paths;

(b) deployment of power equipment, such as uninterruptable power sources, backup diesel generators with fuel tanks; and

(c) implementation of redundant cooling equipment (e.g. cooling towers, chilled water supply and computer room air conditioning units) to control the temperature and humidity levels in the DC and prevent fluctuations potentially harmful to systems.

8.5.3 As part of the DC's environmental controls, the FI should implement fire detection and suppression devices or systems, such as smoke or heat detectors, inert gas suppression systems, and wet or dry sprinkler systems.

8.5.4 The FI's secondary or disaster recovery DC should be geographically separated from its primary or production DC so that both sites will not be impacted by a disruption to the underlying infrastructure (e.g. telecommunications and power) in a particular location.

8.5.5 The DC's physical security and environmental controls should be monitored on a 24 by 7 basis. Appropriate escalation, response plans and procedures for physical and environmental incidents at DCs should be established and tested.

8.5.6 The DC should have adequate physical access controls including:

(a) access granted to staff should be on a need-to-have basis, and revoked promptly if access is no longer required;

(b) proper notification and approval for visitors to the DC. All visitors should be escorted by authorised staff at all times while in the DC;

(c) physical access points in the DC should be secured and monitored at all times;

(d) access to equipment racks should be restricted to authorised staff and monitored;

(e) access to keys and other physical access devices should be restricted to authorised staff, and replaced or changed promptly if they have been misplaced, lost or stolen; and

(f) segregation of delivery and common areas from security sensitive areas should be enforced.

9 Access Control

9.1 User Access Management

9.1.1 The principles of 'never alone',[15] 'segregation of duties',[16] and 'least privilege'[17] should be applied when granting staff access to information assets so that no one person has access to perform sensitive system functions.[18] Access rights and system privileges should be granted according to the roles and responsibilities of the staff, contractors and service providers.

9.1.2 The FI should establish a user access management process[19] to provision, change and revoke access rights to information assets. Access rights should be authorised and approved by appropriate parties, such as the information asset owner.

9.1.3 For proper accountability, the FI should ensure records of user access and user management activities are uniquely identified and logged for audit and investigation purposes.

[15] Certain system functions and procedures are of sensitive and critical nature, and are carried out by more than one person at the same time or performed by one person and checked by another.

[16] Segregation of duties is to ensure that responsibilities and duties for IT functions, such as operating system function, system design and development, application maintenance programming, access control administration, data security, and backup are separated and performed by different groups of employees.

[17] Access rights and system privileges are granted based on job responsibility and the necessity to have them to fulfil one's duties. No person by virtue of rank or position is given any intrinsic right to access confidential data, applications, system resources or facilities. Only personnel with proper authorisation are granted access to and use of information assets.

[18] The sensitivity of a system function may be assessed based on the confidentiality of the data and criticality of the system. This could include system functions that are of a sensitive nature, such as system initialisation, PIN generation, creation of cryptographic keys and the use of administrative accounts.

[19] User access refers to access by all users, including end or business user accounts as well as administrative accounts.

9.1.4 The FI should establish a password policy and a process to enforce strong password controls[20] for users' access to IT systems.

9.1.5 Multi-factor authentication[21] should be implemented for users with access to sensitive system functions to safeguard the systems and data from unauthorised access.

9.1.6 The FI should ensure appropriate parties such as information asset owners perform periodic user access review to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as inappropriate access rights. Exceptions noted from the user access review should be resolved as soon as practicable.

9.1.7 Users should only be granted access rights on a need-to-use basis. Access rights that are no longer needed, as a result of a change in a user's job responsibilities or employment status (e.g. transfer or termination of employment), should be revoked or disabled promptly.

9.1.8 The FI should subject its service providers, who are given access to the FI's information assets, to the same monitoring and access restrictions on the FI's personnel.

9.2 Privileged Access Management

9.2.1 Users granted privileged system access have the ability to inflict severe damage on the stability and security of the FI's IT environment. Access to privileged accounts should only be granted on a need-to-use basis; activities of these accounts should be logged and reviewed as part of the FI's ongoing monitoring.

[20] Strong password controls should include a change of password upon first logon, minimum password length and history and password complexity.

[21] Multi-factor authentication refers to the use of two or more factors to verify a user's claimed identity. Such factors include, but are not limited to:
(a) something that the user knows such as a password or a PIN
number;
(b) something that the user has such as a cryptographic identification device or token; and
(c) something that the user is such as his biometrics or behaviour.

9.2.2 System and service accounts are used by operating systems, applications and databases to interact or access other systems' resources. The FI should establish a process to manage and monitor the use of system and service accounts for suspicious or unauthorised activities.

9.3 Remote Access Management

9.3.1 Remote access allows users to connect to the FI's internal network via an external network to access the FI's data and systems, such as emails and business applications. Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorised access to the FI's IT environment.

9.3.2 The FI should ensure remote access to the FI's information assets is only allowed from devices that have been secured according to the FI's security standards.

10 Cryptography

10.1 Cryptographic Algorithm and Protocol

10.1.1 The primary applications of cryptography are to protect data confidentiality, and maintain data integrity and authenticity. For example, cryptography is used in data encryption to protect sensitive data; cryptographic digital signatures can be used to verify the authenticity of the data origin and check if the data has been altered. Besides these applications, cryptography is also commonly used in authentication protocols.

10.1.2 The FI should adopt cryptographic algorithms from well-established international standards. The FI should also select an appropriate algorithm and encryption key length that meet its security objectives and requirements.

10.1.3 Where the security of the cryptographic algorithm depends on the unpredictability of a random seed or number, the FI should ensure the seed or random number is of sufficient length and randomness.

10.1.4 The FI should ensure all cryptographic algorithms used have been subject to rigorous testing or vetting to meet the identified security objectives and requirements.

10.1.5 The FI should monitor developments in the area of cryptanalysis and, where necessary, update or change the cryptographic algorithms or increase the key lengths to ensure they remain resilient against evolving threats.

10.2 Cryptographic Key Management

10.2.1 Cryptographic key management policy, standards and procedures covering key generation, distribution, installation, renewal, revocation, recovery and expiry should be established.

10.2.2 The FI should ensure cryptographic keys are securely generated and protected from unauthorised disclosure. Any cryptographic key or sensitive data used to generate or derive the keys should be also be protected or securely destroyed after the key is generated.

10.2.3 The FI should determine the appropriate lifespan of each cryptographic key based on factors, such as the sensitivity of the data, the criticality of the system to be

protected, and the threats and risks that the data or system may be exposed to. The cryptographic key should be securely replaced, before it expires at the end of its lifespan.

10.2.4 To protect sensitive cryptographic keys, the FI should manage, process and store such keys in hardened and tamper resistant systems, e.g. by using a hardware security module.

10.2.5 Where sensitive cryptographic keys need to be transmitted, the FI should ensure these keys are not exposed during transmission. The keys should be distributed to the intended recipient via an out-of-band channel or other secure means to minimise the risk of interception.

10.2.6 Diversification of cryptographic keys can limit the impact of key exposure. Cryptographic keys should be used for a single purpose. For instance, the cryptographic key for data encryption should be different from the one that is used to generate cryptographic digital signatures.

10.2.7 If a cryptographic key is found to be compromised, the FI should revoke and replace the key and all other keys whose security could also be compromised as a result of the exposed key.

10.2.8 When cryptographic keys have expired or have been revoked, the FI should use a secure key destruction method to ensure the keys are not recoverable.

10.2.9 When replacing or renewing a compromised or expiring cryptographic key, the FI should generate the new key in a manner such that any adversary who has knowledge of part or whole of the previous key will not be able to derive the new key from it.

10.2.10 Cryptographic keys can be corrupted or unintentionally deleted. As such, the FI should maintain backups of cryptographic keys for recovery purposes and accord them a high level of protection.

11 Data and Infrastructure Security

11.1 Data Security

11.1.1 The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data, taking into consideration the following:

(a) data in motion - data that traverses a network or that is transported between sites;

(b) data at rest - data in endpoint devices such as notebooks, personal computers, portable storage devices and mobile devices, as well as data in systems such as files stored on servers, databases, backup media and storage platforms (e.g. cloud); and

(c) data in use - data that is being used or processed by a system.

11.1.2 The FI should implement appropriate measures to prevent and detect data theft, as well as unauthorised modification in systems and endpoint devices. The FI should ensure systems managed by the FI's service providers are accorded the same level of protection and subject to the same security standards.

11.1.3 Systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in systems and endpoint devices should be encrypted and protected by strong access controls.

11.1.4 The FI should ensure only authorised data storage media, systems and endpoint devices are used to communicate, transfer, or store confidential data.

11.1.5 Security measures should be implemented to prevent and detect the use of unauthorised internet services which allow users to communicate or store confidential data. Examples of such services include social media, cloud storage and file sharing, emails, and messaging applications.

11.1.6 The use of sensitive production data in non-production environments should be restricted. In exceptional situations where such data needs to be used in non-production environments, proper approval has to be obtained from senior management. The FI

should ensure appropriate controls are implemented in non-production environments to manage the access and removal of such data to prevent data leakage. Where possible, such data should be masked in the non-production environments.

11.1.7 The FI should ensure confidential data is irrevocably deleted from storage media, systems and endpoint devices before they are disposed of or redeployed.

11.2 Network Security

11.2.1 The FI should install network security devices such as firewalls to secure the network between the FI and the Internet, as well as connections with third parties.

11.2.2 To minimise the risk of cyber threats, such as lateral movement and insider threat, the FI should deploy effective security mechanisms to protect information assets. Information assets could be grouped into network segments based on the criticality of systems, the system's functional role (e.g. database and application) or the sensitivity of the data.

11.2.3 Network intrusion prevention systems should be deployed in the FI's network to detect and block malicious network traffic.

11.2.4 The FI should implement network access controls to detect and prevent unauthorised devices from connecting to its network.

11.2.5 Network access control rules in network devices such as firewalls, routers, switches and access points should be reviewed on a regular basis to ensure they are kept up-to-date. Obsolete rules and insecure network protocols should be removed promptly as these can be exploited to gain unauthorised access to the FI's network and systems.

11.2.6 Internet web browsing provides a conduit for cyber criminals to access the FI's IT systems. In this regard, the FI should consider isolating internet web browsing activities from its endpoint devices through the use of physical or logical controls, or implement equivalent controls, so as to reduce exposure of its IT systems to cyber attacks.

11.2.7 An effective DoS protection should be implemented to detect and respond to various types of DoS attacks.[22] The FI could engage DoS mitigation service providers to filter potential DoS traffic before it reaches the FI's network infrastructure.

11.2.8 A review of the FI's network architecture, including the network security design, as well as system and network interconnections, should be conducted on a periodic basis to identify potential cyber security vulnerabilities.

11.3 System Security

11.3.1 The security standards for the FI's hardware and software (e.g. operating systems, databases, network devices and endpoint devices) should outline the configurations that will minimise their exposure to cyber threats. The standards should be reviewed periodically for relevance and effectiveness.

11.3.2 The FI should establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely manner.

11.3.3 Endpoint protection, which includes but is not limited to behavioural-based and signature-based solutions, should be implemented to protect the FI from malware infection and address common delivery channels of malware, such as malicious links, websites, email attachments or infected removable storage media.

11.3.4 The FI should ensure that anti-malware signatures are kept up-to-date and the systems are regularly scanned for malicious files or anomalous activities.

11.3.5 To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform scanning of indicators of compromise (IOCs) in a timely manner, and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities.

[22] The types of DoS attacks to be considered should include distributed, volumetric and application layer attacks.

11.3.6 Security measures, such as application white-listing, should be implemented to ensure only authorised software is allowed to be installed on the FI's systems.

11.3.7 When implementing Bring Your Own Device (BYOD)[23], the FI should conduct a comprehensive risk assessment and implement appropriate measures to secure its BYOD environment before allowing staff to use their personal devices to access the corporate network. Refer to Annex B on the security measures for BYOD.

11.4 Virtualisation Security

11.4.1 Virtualisation [24] is used by organisations to optimise the use of computing resources and to enhance resilience. The technology allows several virtual machines (VMs) that support different business applications to be hosted on a physical system. A system failure or security breach in one of the VMs could have contagion impact on other VMs. The FI should ensure security standards are established for all components[25] of a virtualisation solution.

11.4.2 Strong access controls should be implemented to restrict administrative access to the hypervisor and host operating system as both control the guest operating systems and other components in the virtual environment.

11.4.3 The FI should establish policies and standards to manage virtual images and snapshots. The standards should include details that govern the security, creation, distribution, storage, use, retirement and destruction of virtual images and snapshots so as to protect these assets against unauthorised access or modification.

[23] BYOD enables staff to access corporate email, calendars, applications and data from their personal mobile devices.

[24] Virtualisation is the simulation of the software or hardware upon which other software runs. This simulated environment is called a virtual machine. Adapted from NIST SP800 125, *Guide to Security for Full Virtualisation Technologies,* January 2011.

[25] Components of a virtualisation solution typically include the hypervisor, the host operating system and the guest operating system.

11.5 Internet of Things

11.5.1 Internet of Things (IoT) includes any electronic devices, such as smart phones, multi-function printers, security cameras and smart televisions, which can be connected to the FI's network or the Internet. As with all information assets, the FI should maintain an inventory of all its IoT devices, including information such as the networks which they are connected to and their physical locations.

11.5.2 Many IoT devices are designed without or with minimal security controls. If compromised, these devices can be commandeered and used to gain unauthorised access to the FI's network and systems or as a launch pad for cyber attacks on the FI. The FI should assess and implement processes and controls to mitigate risks arising from IoT.

11.5.3 The network that hosts IoT devices should be secured. For instance, network access controls can be implemented to restrict network traffic to and from an IoT device to prevent a cyber threat actor from accessing the FI's network and launching malware or DoS attacks. To further reduce IoT risks, the FI should host IoT devices in a separate network segment from the network that hosts the FI's systems and confidential data.

11.5.4 The FI should implement controls to prevent unauthorised access to IoT devices.

11.5.5 Similar to other systems, the FI should monitor IoT devices for suspicious or anomalous system activities so that prompt actions can be taken to isolate compromised devices.

12 Cyber Security Operations

12.1 Cyber Threat Intelligence and Information Sharing

12.1.1 To maintain good cyber situational awareness, the FI should establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the FI's business and IT environment. Cyber-related information would include cyber events, cyber threat intelligence and information on system vulnerabilities.

12.1.2 The FI should procure cyber intelligence monitoring services. As cyber threat information sharing is an important component of cyber resilience within the financial ecosystem, the FI should actively participate in cyber threat information-sharing arrangements with trusted parties to share and receive timely and actionable cyber threat information.

12.1.3 At the same time, the FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the Internet. The FI should consider engaging external media monitoring services to facilitate the evaluation and identification of online misinformation.

12.2 Cyber Event Monitoring and Detection

12.2.1 To facilitate continuous monitoring and analysis of cyber events;[26] as well as prompt detection and response to cyber incidents, the FI should establish a security operations centre or acquire managed security services. The processes, roles and responsibilities for security operations should be defined.

12.2.2 A process to collect, process, review and retain system logs[27] should be established to facilitate the FI's security monitoring operations. These logs should be protected against unauthorised access.

[26] Cyber events include exploits on system vulnerabilities, system intrusions, privileged escalation, unauthorised system access, data exfiltration and attempts to establish connections via the Internet to Command and Control (C2) servers.

[27] These include security, application, database, network and operating system logs.

12.2.3 To facilitate identification of anomalies, the FI should establish a baseline profile of each IT system's routine activities and analyse the system activities against the baseline profiles. The profiles should be regularly reviewed and updated.

12.2.4 The FI should consider applying user behavioural analytics to enhance the effectiveness of security monitoring. User behavioural analytics might include the use of machine learning algorithms in real time to analyse system logs, establish a baseline of normal user activities and identify suspicious or anomalous behaviours.

12.2.5 Correlation of multiple events registered on system logs should be performed to identify suspicious or anomalous system activity patterns.

12.2.6 A process should be established to ensure timely escalation to relevant stakeholders regarding suspicious or anomalous system activities or user behaviour.

12.3 Cyber Incident Response and Management

12.3.1 The FI should establish a cyber incident response and management plan to swiftly isolate and neutralise a cyber threat and to securely resume affected services. The plan should describe communication, coordination and response procedures to address plausible cyber threat scenarios.

12.3.2 As part of the plan, the FI should establish a process to investigate and identify the security or control deficiencies that resulted in the security breach. The investigation should also evaluate the full extent of the impact to the FI.

12.3.3 Information from cyber intelligence and lessons learnt from cyber incidents should be used to enhance the existing controls or improve the cyber incident management plan.

13 Cyber Security Assessment

13.1 Vulnerability Assessment

13.1.1 The FI should establish a process to conduct regular vulnerability assessment (VA) on their IT systems to identify security vulnerabilities and ensure risk arising from these gaps are addressed in a timely manner. The frequency of VA should be commensurate with the criticality of the IT system and the security risk to which it is exposed.

13.1.2 When performing VA, the scope should minimally include vulnerability discovery, identification of weak security configurations, and open network ports, as well as application vulnerabilities. For web-based systems, the scope of VA should include checks on common web-based vulnerabilities.

13.2 Penetration Testing

13.2.1 The FI should carry out penetration testing (PT) [28] to obtain an in-depth evaluation of its cyber security defences. A combination of blackbox and greybox testing should be conducted for online financial services.

13.2.2 A bug bounty programme is another means by which an FI could discover vulnerabilities in their IT systems by inviting and incentivising ethical or "white hat" hackers to conduct PT on their systems. The FI may consider conducting a bug bounty programme to test the security of its IT infrastructure to complement its PT.

13.2.3 To obtain a more accurate assessment of the robustness of the FI's security measures, PT should be conducted on the production environment. Proper safeguards should be implemented when PT is conducted on the production environment.

13.2.4 The frequency of PT should be determined based on factors such as system criticality and the system's exposure to cyber risks. For systems that are directly accessible

[28] The 2 common types of penetration testing are:

a) blackbox testing, which refers to testing without any prior knowledge of the environment except for the IP address ranges and known URLs; and

b) greybox testing, which refers to testing with credentials. The security assessor is authenticated using the same rights as a normal customer

Adapted from *ABS Penetration Testing Guidelines for the Financial Industry in Singapore*, 31 July 2015.

from the Internet, the FI is expected to conduct PT to validate the adequacy of the security controls at least once annually or whenever these systems undergo major changes or updates.

13.3 Cyber Exercises

13.3.1 The FI should carry out regular scenario-based cyber exercises to validate its response and recovery, as well as communication plans against cyber threats. These exercises could include social engineering,[29] table-top,[30] or cyber range[31] exercises.

13.3.2 Depending on the exercise objectives, the FI should involve relevant stakeholders, including senior management, business functions, corporate communications, crisis management team, service providers, and technical staff responsible for cyber threat detection, response and recovery.

[29] Social engineering is a process in which cyber criminals manipulate an unsuspecting person into divulging sensitive details such as passwords through the use of techniques such as phishing, identity theft and spam.

[30] Table-top exercise is a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. Adapted from NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

[31] Cyber ranges are interactive, simulated representations of an organisation's local network, IT system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and secure environment for product development and security posture testing. Adapted from NIST, *Cyber Ranges*, https://www.nist.gov/sites/default/files/documents/2018/02/13/cyber_ranges.pdf

13.4 Adversarial Attack Simulation Exercise

13.4.1 The FI should perform an adversarial attack simulation exercise[32] to test and validate the effectiveness of its cyber defence and response plan against prevalent cyber threats.

13.4.2 The objectives, scope and rules of engagement should be defined before the commencement of the exercise, and the exercise should be conducted in a controlled manner under close supervision to ensure the activities carried out by the red team[33] do not disrupt the FI's production systems.

13.5 Intelligence-Based Scenario Design

13.5.1 To simulate realistic adversarial attacks during any cyber security assessment, the threat scenario should be designed and based on challenging but plausible cyber threats.

13.5.2 The FI could also design the exercise scenario by using threat intelligence that is relevant to their IT environment to identify threat actors who are most likely to pose a threat to the FI; and identify the tactics, techniques and procedures most likely to be used in such attacks.

13.6 Remediation Management

13.6.1 A comprehensive remediation process should be established to track and resolve issues identified from the cyber security assessments or exercises. The process should minimally include the following:

(a) severity assessment and classification of an issue;

[32] Adversarial attack simulation exercise provides a more realistic picture of an FI's capability to prevent, detect and respond to real adversaries by simulating the tactics, techniques and procedures of real-world attackers to target people, processes and technology underpinning the FI's critical business functions or services. Adapted from ABS Guidelines for the Financial Industry in Singapore, *Red Team: Adversarial Attack Simulation Exercises,* version 1, November 2018.

[33] An individual or team designated to simulate the attack techniques, tactics and procedures of a real adversary to reach an objective set in the scope of the adversary simulation exercise.
ABS Guidelines for the Financial Industry in Singapore, *Red Team: Adversarial Attack Simulation Exercises,* version 1, November 2018.

(b) timeframe to remediate issues of different severity; and

(c) risk assessment and mitigation strategies to manage deviations from the framework.

14 Online Financial Services

14.1 Security of Online Financial Services

14.1.1 Online financial services include banking, trading, insurance, or other financial and payment services that are provisioned via the Internet.[34] In delivering online financial services, the FI should implement security and control measures which are commensurate with the risk involved to ensure the security of data and online services.

14.1.2 The FI should secure its communications channels to protect customer data. This can be achieved through data encryption and digital signatures.

14.1.3 Adequate measures should also be taken to minimise exposure of the FI's online financial services to common attack vectors such as code injection attack, cross-site scripting, man-in-the-middle attack (MITMA),[35] domain name system (DNS) hijacking,[36] distributed denial of service (DDoS), malware and spoofing attacks.

14.1.4 An FI offering online financial services access via a mobile device should be aware of the risks unique to mobile applications. Specific measures aimed at addressing the risks of mobile applications should be put in place. Refer to Annex C for guidance on Mobile Application Security.

14.1.5 The FI should only make available mobile applications or software to customers through official mobile application stores, or other secure delivery channels.

[34] Examples of online financial services include online banking, mobile banking, phone banking, online trading, mobile/digital wallets and payments, and financial and payment services offered using account and transaction APIs, etc.

[35] In a MITMA attack, an interloper is able to read, insert and modify messages between two communicating parties without either one knowing that the communication between them has been compromised. Possible attack points for MITMA could be within customer computers, internal networks, information service providers, web servers or anywhere in the Internet along the path between the customer and the FI's server.

[36] A cyber attack technique where an attacker uses malware to change the IP address of a resource linked to a specific domain name (e.g. a particular website), and redirect victims to a rogue domain name (e.g. phishing or fake website).

14.1.6 The FI should actively monitor for phishing campaigns targeting the FI and its customers. Immediate action should be taken to report phishing attempts to service providers to facilitate the removal of malicious content. The FI should alert its customers of such campaigns and advise them of security measures to adopt to protect against phishing.

14.1.7 Rooted or jailbroken mobile devices, which are more susceptible to malware and may have more security vulnerabilities, should be disallowed from accessing the FI's mobile applications to perform financial transactions unless the application has been secured within a sandbox or container that insulates the application from tampering and interception by malware.

14.2 Customer Authentication and Transaction Signing

14.2.1 Multi-factor authentication should be deployed at login for online financial services to secure the customer authentication process. Multi-factor authentication can be based on two or more of the following factors, i.e. what you know (e.g. personal identification number or password), what you have (e.g. one-time password (OTP) generator) and who you are (e.g. biometrics).

14.2.2 End-to-end encryption should be implemented for the transmission of customer passwords so that they are not exposed at any intermediate nodes between the customer mobile application or browser and the IT system where passwords are verified. To safeguard the confidentiality of customer passwords, the passwords should only be verified in a hardened or tamper resistant system.

14.2.3 The FI should implement transaction-signing (e.g. digital signatures) for authorising high-risk activities to protect the integrity of customer accounts' data and transaction details. High-risk activities include changes to sensitive customer data (e.g. customer office and home address, email and telephone contact details), registration of third party payee details, high value funds transfers and revision of funds transfer limits.

14.2.4 Besides login and transaction-signing for high-risk activities, the FI may implement appropriate risk-based or adaptive authentication that presents customers with authentication options that are commensurate with the risk level of the transaction and sensitivity of the data.

14.2.5 When implementing time-based OTPs, the FI should establish a validity period that is as short as practicable to lower the risk of a stolen OTP being used for fraudulent transactions.

14.2.6 Where biometric technologies[37] and customer passwords are used for customer authentication, the FI should ensure the biometrics-related data and authentication credentials are encrypted in storage and during transmission.

14.2.7 The performance of the biometric solution, based on false acceptance rate (FAR)[38] and false rejection rate (FRR),[39] should be calibrated to be commensurate with the risk associated with the online activity.

14.2.8 A soft token is a software-based two-factor authentication mechanism installed on a general-purpose device.[40] Appropriate measures, such as verifying the identity of the customer, detecting and blocking rooted or jailbroken devices, and performing device binding,[41] should be implemented during soft token provisioning.

14.2.9 The FI should ensure the authenticated session, together with its encryption protocol, remains intact throughout the interaction with the customer. Measures to detect and terminate hijacked sessions should be implemented. To reduce the risk of an attacker from maintaining a hijacked session indefinitely, an online session should be automatically terminated after inactivity for a pre-defined time.

14.2.10 Where alternate controls and processes (e.g. maker-checker function) are implemented for corporate or institutional customers to authorise transactions, the FI should perform a security risk assessment of controls or processes to ensure they are commensurate with the risk of the activities that are being carried out.

14.2.11 To safeguard the confidentiality of authentication credentials, such as biometric templates and passwords, the FI should store these credentials in a form that is resistant

[37] Biometric recognition technologies could be based on face, iris or palm images, voice patterns, etc.

[38] FAR represents the instance a biometric identification solution positively verifies an unauthorised person.

[39] FRR represents the instance a biometric identification solution fails to verify an authorised person correctly.

[40] Examples: a desktop computer, laptop, or mobile device like a smartphone or tablet.

[41] Device binding is a technique to link an authorised user to his registered device and ensure accountability.

to reverse engineering. A process and procedure should also be implemented to revoke and replace authentication credentials and mechanisms that have been compromised.

14.3 Fraud Monitoring

14.3.1 The FI should implement real-time fraud monitoring systems to identify and block suspicious or fraudulent online transactions.[42]

14.3.2 A process should be established to investigate suspicious transactions or payments and to ensure issues are adequately and promptly addressed.

14.3.3 The FI should notify customers of suspicious activities or funds transfers above a threshold that is defined by the FI or customers. The notification should contain meaningful information such as type of transaction and payment amount, as well as instructions to report suspicious activities or unauthorised transactions.

14.4 Customer Education and Communication

14.4.1 Customers should be informed of the security best practices that they should adopt when using online financial services. This includes the measures to take to secure their electronic devices that are used to access online financial services.

14.4.2 The FI should alert its customers on a timely basis to new cyber threats so that they can take precautionary measures.

14.4.3 The FI should advise their customers on the means to detect unauthorised transactions and to report promptly security issues, suspicious activities or suspected fraud to the FI.

[42] For example, transactions or payments exhibiting behaviour which deviates significantly from a customer's usual usage behaviours, or abnormal system activities (e.g. multiple sessions using an identical customer account originating from different geographical locations within a short time span).

15 IT Audit

15.1 Audit Function

15.1.1 Audit plays an important role to assess the effectiveness of the controls, risk management and governance process in the FI. The FI should ensure IT audit is performed to provide the board of directors and senior management an independent and objective opinion of the adequacy and effectiveness of the FI's risk management, governance and internal controls relative to its existing and emerging technology risks.

15.1.2 A comprehensive set of auditable areas for technology risk should be identified so that an effective risk assessment could be performed during audit planning. Auditable areas should include all IT operations, functions and processes.

15.1.3 The frequency of IT audits should be commensurate with the criticality of and risk posed by the IT information asset, function or process.

15.1.4 The FI should ensure its IT auditors have the requisite level of competency and skills to effectively assess and evaluate the adequacy of IT policies, procedures, processes and controls implemented.

Annex A: Application Security Testing

A.1 Application security testing aims to identify and remediate exploitable loopholes and weaknesses in software applications that could result in data leakage, disruption to business operations, financial losses and reputational damage. A good application security testing practice requires proactive security assurance techniques to be built into the various phases of the SDLC.

A.2 Common testing methods for identifying security vulnerabilities in software applications include:

(a) Static Application Security Testing

Static Application Security Testing (SAST) involves a set of tools or technologies designed to scan and analyse static source codes, byte codes and binaries for coding and design flaws indicative of security vulnerabilities. The tester will have full internal knowledge of the IT system including architecture and design specifications, source codes or configuration files to guide the testing.

(b) Dynamic Application Security Testing

Dynamic Application Security Testing (DAST) involves a set of tools or technologies designed to detect conditions indicative of exploitable vulnerabilities in an IT system in its run-time state. The tester has limited or no prior knowledge of the system when the test is performed.

(c) Interactive Application Security Testing

Interactive Application Security Testing (IAST) involves a combination of SAST and DAST techniques to analyse application codes, run-time controls libraries, requests and responses, as well as data and control flows and identify vulnerabilities in an IT system.

(d) Fuzzing or Fuzz Testing

Fuzzing is an automated software testing technique used to discover coding errors and bugs by inputting random data, known as fuzz, to the IT system. This could be included as part of DAST or IAST.

Annex B: BYOD Security

B.1 The FI should implement data loss prevention measures on personal computing or mobile devices that are used to access the FI's information assets. Two common ways to address BYOD security are the use of mobile device or application management, as well as virtualisation solutions. These solutions can be augmented with other security measures for personal devices to provide enhanced functionalities:

(a) Mobile Device or Application Management

Mobile Device Management (MDM) solutions are used to manage and control mobile devices used to access the FI's resources while Mobile Application Management (MAM) are used to manage and control the access at the application. Before a personal device or application is permitted to access the FI's network, the device is verified to ensure it has not been "jailbroken", "rooted" or compromised. MDM and MAM solutions usually come with storage encryption, "lock and wipe" capabilities, enforced authentication policies and can be used in conjunction with other security measures.

(b) Virtualisation

Virtualisation allows staff to have on-demand access to enterprise computing resources and data from their personal devices. Strict security policies should be enabled within the virtual environment to restrict copying and use of peripheral devices, such as printers and removable attached storage, to prevent data leakage.

Annex C: Mobile Application Security

C.1 Security measures that should be considered for securing mobile applications are as follows:

(a) avoid storing or caching data in the mobile application to mitigate the risk of data compromise on the device. Data should be stored in a protected and trusted area of the mobile device;

(b) protect private cryptographic keys;

(c) implement anti-hooking or anti-tampering mechanisms to prevent injection of malicious code that could alter or monitor the behaviour of the application at runtime;

(d) implement appropriate application integrity check (e.g. using checksum and digital signature) to verify the authenticity and integrity of the application and code obfuscation techniques to prevent reverse engineering of the mobile application;

(e) implement certificate or public key pinning to protect against MITMA;

(f) implement a secure in-app keypad to mitigate against malware that captures keystrokes; and

(g) implement device binding to protect the software token from being cloned.

Monetary Authority of Singapore