CONSULTATION PAPER

P003 - 2019

March 2019

Technology Risk Management Guidelines

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. Financial institutions (FIs) are riding the wave of digital transformation to increase efficiency in their operations and to deliver better financial services to consumers.

1.2 FIs aim to deliver innovative services, partner with financial technology (FinTech) companies and actively explore open banking[1] strategies to stay competitive and provide customers with better and more efficient online financial services. While digital transformation expands the options and accessibility of financial services to consumers, they also increase FIs' exposure to a range of operational risks, including technology risks, which could lead to operational disruptions and data breaches. In this regard, FIs should fully understand the magnitude of technology risks and put in place adequate and robust risk management systems, as well as operating processes to manage these risks.

1.3 The cyber threat landscape is evolving and cyber criminals' techniques are becoming increasingly sophisticated with the use of encryption and advanced technologies, such as data analytics. Cyber criminals tend to target the weak links in the interconnected financial ecosystem to carry out fraudulent financial transactions, exfiltrate sensitive financial data or disrupt systems that support financial services. Hence, every FI has an important role to play in building a cyber resilient financial sector.

1.4 The MAS Technology Risk Management Guidelines published in 2013 set out technology risk management principles and best practices for the financial sector. They have been updated with greater focus in the following key areas:

(a) 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 proposed revisions articulate the need for both the FI's board of directors and senior management

[1] Open banking broadly captures the concept that a consumer owns information about himself, and should be able to share that information with any third party if he chooses, for example through APIs, and to transfer his money to any third party seamlessly.

to have members with the necessary skills and understanding of technology risks. The responsibilities of the board of directors and senior management also include establishing a strong risk culture and a sound and robust technology risk management framework.

(b) Software Development and Management

Many FIs have adopted Agile development methods and DevOps practices to facilitate rapid software delivery. The proposed revisions advocate the adoption of secure software development best practices, such as secure coding and code review when using Agile development methods and enforcement of segregation of duties in key DevOps practices.

(c) Emerging Technologies

FIs are increasingly investing in technologies, such as APIs, smart electronic devices and virtualisation, to improve service delivery and efficiency. If they are not implemented and managed appropriately, these technologies may increase the cyber attack surface. Additional guidance is included to manage risks arising from such technologies.

(d) Cyber Resilience

Strong cyber resilience is critical to sustaining trust and confidence in financial services. The frequency and impact of cyber incidents have increased in recent years. The guidelines support a defence-in-depth approach to strengthening cyber resilience. The proposed revisions include guidance on cyber surveillance, cyber security assessment and testing, as well as cyber incident management. It is important that FIs establish and continuously strengthen the processes and controls to identify, prevent, detect, respond to and recover from cyber incidents.

1.5 The MAS circulars issued after July 2013 on vulnerability assessment and penetration testing, IT security risks posed by personal mobile devices, early detection of cyber intrusions and technology risk, and cyber security training for the FI's board of directors have been incorporated into the revised guidelines to facilitate ease of reference by users.

1.6 MAS invites comments from FIs and other interested parties on the revised guidelines.

Please note that all submissions received will be published and attributed to the respective respondents unless they expressly request MAS not to do so. As such, if respondents would like:

(i) their whole submission or part of it (but not their identity), or

(ii) their identity along with their whole submission,

to be kept confidential, please expressly state so in the submission to MAS. MAS will only publish non-anonymous submissions. In addition, MAS reserves the right not to publish any submission received where MAS considers it not in the public interest to do so, such as where the submission appears to be libellous or offensive.

1.7 Please submit your comments via the online submission form by **8 April 2019**.

1.8 If you have any queries, please email techrisk@mas.gov.sg.

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 practices for the management of technology risk. FIs are expected to implement the measures that are relevant to their operating environment.

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 FIs are reliant on technology to enable its business and to deliver financial services. It is vital that the FIs' board of directors and senior management ensure effective internal controls, and risk management practices are implemented and maintained to achieve security, reliability and resilience.

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

3.1.3 The board of directors and senior management should be involved in key IT decisions that may change the FI's risk appetite and strategy.

3.1.4 If not managed well, technology risk will have an extensive impact on business. Hence, the board of directors and senior management should set the tone from the top and cultivate a strong culture of technology risk management and awareness at all levels of staff within the FI.

3.1.5 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 in a manner that is commensurate with the FI's risks;

(b) ensuring appropriate governance structures and processes, with well-defined roles, responsibilities, and clear reporting lines across the various organisational functions are established;

(c) appointing a Chief Information Officer, Chief Technology Officer or Head of Information Technology with the requisite expertise and experience, to be responsible for information technology and computer systems that support enterprise goals;

(d) appointing a Chief Information Security Officer or Head of Information Security, with the requisite expertise and experience, to be responsible for the FI's IT security strategy and programme;

(e) 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;

(f) setting a suitable risk appetite for the type and extent of technology risks the FI is willing and able to assume;

(g) endorsing the FI's technology risk management strategy;

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

(i) ensuring adequate resources and expertise are assigned to implement and enforce the strategy; and

(j) assessing management competencies for developing policies to manage technology risks.

3.1.6 Senior management is responsible for:

(a) managing technology risks based on the framework approved by the board of directors;

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

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

(d) ensuring the effectiveness of policies, standards and procedures to reflect changes in managing the FI's risk environment;

[2] The roles and responsibilities of senior management and staff could be defined and tracked using a Responsibility Assignment Matrix[2], 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.

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

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

3.2 Policies, Standards and Procedures

3.2.1 The FI should establish policies, standards and procedures and, where appropriate, incorporate industry standards 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 assessed, reviewed and approved by senior management. Approved deviations should be reviewed periodically to ensure the attendant 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 to ensure compliance deviations are identified, monitored, addressed and remediated in a timely manner.

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 an information asset management framework that includes the following:

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

[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) establishment of the 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[4] services by FIs may not constitute outsourcing. However, as many of these services are provisioned or delivered using IT or may involve confidential customer information being held by the third party, the FI and its customers may be adversely impacted if there is a system failure or security breach at the third party. Hence, the FI should conduct an assessment of these services' exposure to various technology risks associated with the loss of data confidentiality, integrity and service availability, and manage these associated risks.

3.4.2 Proper due diligence should be carried out by the FI to determine the service provider's financial viability, track record, reliability and capability, including relevant certification or accreditation that is recognised by the industry, before entering into a contractual agreement or partnership with the service provider.

[4] Third party is understood as a broad sense, including: (i) all forms of outsourcing (including cloud computing services); (ii) standardised and non-standardised services and products that are typically not considered outsourcing (power supply, telecommunications lines, commercial hardware and software, etc.); and (iii) interconnected counterparties such as other institutions (financial or not) and FMIs (e.g. payment and settlement systems, trading platforms, central securities depositories and central counterparties). Adapted from Basel Committee on Banking Supervision, *Cyber Resilience: Range of Practices*, December 2018.

3.5 Competency and Background Review

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

3.5.2 Insider threat, which may involve theft of confidential data, sabotage of systems or fraud by staff, contractors and services providers, is considered one of the key risks to an organisation. A background check on personnel, who has access to the FI's data and 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 IT security awareness of 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 and deployment 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 training programme should be extended to the board of directors to raise their awareness on risks associated with the use of technology and enhance their understanding of technology risk management practices. The training programme for the board of directors may comprise briefings by in-house technology risk professionals or external specialists.

3.6.4 To ensure the training remain current and relevant, the training programme and its effectiveness should be reviewed periodically, taking into consideration changes in the FI's IT security policies, prevalent and emerging risks, and the evolving 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 in a consistent and systematic manner. As part of the framework, effective risk management practices and internal controls should be instituted to achieve data confidentiality[5] and integrity, system security and reliability, as well as resilience in its IT operating environment.

4.1.2 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 risk owner may be assumed by a function or group of functions within the FI, who is accountable and given the authority to manage technology risks.

4.1.3 The framework should encompass the following components:

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

(b) risk assessment – assess the potential impact and likelihood of current and emerging threats 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, systems, environmental or operating conditions; and report key risks to the board of directors and senior management.

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

4.1.4 Due to changes in the FI's business and IT environment, as well as the evolving cyber threat landscape, FIs 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[6] and vulnerabilities, as well as the risks[7] posed to its IT environment, including information assets that are maintained or supported by third party service providers.

4.2.2 Security threats such as internal sabotage, malware, data theft and unauthorised financial transactions could have a severe impact on an FI and its stakeholders. The FI should be vigilant in monitoring these threats as it is a crucial step towards containing the risks.

4.3 Risk Assessment

4.3.1 Following risk identification, the FI should perform an analysis and quantification of the potential impact and consequences of these risks on the overall business and operations. The extent of risk depends on the likelihood of various threats in causing harm to the FI, and its impact should an adverse event occur.

4.3.2 To facilitate the FI in prioritising technology risks, a set of criteria measuring and determining the likelihood and impact of threats and vulnerabilities should be established. The FI should take into consideration financial, operational, legal, reputational and regulatory factors in assessing technology risks.

[6] A threat may take the form of any condition, circumstance, incident or person with the potential to cause harm by exploiting a vulnerability in a system. The source of the threat can be natural, human or environmental. Humans are significant sources of threats through deliberate acts or omissions which could inflict extensive harm to the organisation and its IT systems.

[7] These include risks to the FI's customers, counterparties or other dependent third parties.

4.4 Risk Treatment

4.4.1 For each type of risk identified, the FI should develop and implement risk mitigation and control strategies that are consistent with the value of the information assets and the level of risk tolerance.

4.4.2 Risk mitigation entails a methodical approach for evaluating, prioritising and implementing appropriate risk-reduction controls. The FI should also assess its risk tolerance for damages and losses in the event that a given risk-related event materialises.

4.4.3 As it may not be practical to address all known risks simultaneously or in the same timeframe, the FI should give priority to threats and vulnerabilities with a higher risk rating, such that those which could cause significant harm or impact to the FI's information assets and operations.

4.4.4 The FI should manage and control risks in a manner that will maintain its financial and operational viability and stability. When deciding on the controls and security measures to adopt, the FI should assess the effectiveness of the controls and security measures with regard to the risks being mitigated.

4.4.5 The FI should refrain from implementing a system or acquiring an IT service where threats to the safety and soundness of the FI cannot be adequately controlled and the risks out-weigh the benefits.

4.4.6 To mitigate risks, the FI could consider taking insurance cover for various insurable technology risks, including recovery and restitution costs.

4.4.7 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 controls and security measures. The criteria for risk acceptance should be clearly defined and it should commensurate with the FI's risk tolerance. Acceptable or residual risks should be formally endorsed by the senior management and monitored.

4.4.8 IT control and risk mitigation approach should be subjected to regular review and update, taking into account changing threat landscape and variations in the FI's risk profile.

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 could consider risk events and audit observations, as well as refer to 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. In system development projects, standards and procedures for the different phases of the system development life cycle[8] (SDLC) should be maintained.

5.1.4 As project risks, such as an ill-defined project scope and poor cost management, 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. For large and complex projects that impact the business, the FI should report significant project risks to its board of directors and senior management.

5.2 Project Steering Committee

5.2.1 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.

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

5.2.2 Issues or problems 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 The FI should ensure the vendor puts in place robust software development and quality assurance practices, as well as stringent security practices to safeguard and protect any sensitive data the vendor has access to over the course of the project. Similarly, any vendor access to the FI's systems should be tightly controlled and monitored.

5.3.3 If the project involves commercial off-the-shelf solution that does not meet the FI's 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 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.

5.4 System Development Life Cycle and Security-By-Design

5.4.1 The FI should establish a framework to manage its SDLC. The framework should clearly define the processes, procedures and controls in each phase in the life cycle (e.g. initiation/planning, requirements analysis, design, implementation, testing and acceptance, etc.)

5.4.2 The security-by-design principle requires the design and implementation of security in every phase of the SDLC in order to develop IT system that is reliable and resilient to attacks. This includes incorporation of security specifications in the system design, continuous security evaluation and adherence to security practices throughout the SDLC. The principle should be adhered to such that security requirements are clearly specified in the early phase of system development. The 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.

5.4.3 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 system. In addition to functional requirements, key requirements such as system performance, resiliency 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 system, and determine the 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 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 use track and 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 system should be reviewed by the IT security function or a qualified security consultant.

5.7 System Testing and Acceptance

5.7.1 A methodology for system testing[9] should be established. The scope of tests 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.

[9] System testing is broadly defined to include 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 an appropriate test case in the relevant test plan.

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 system to validate that the system 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 to 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, and achieve the project objectives.

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 hackers 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 establish standards on secure coding, source code review[10] and application security testing, and ensure the standards are applied and adopted throughout the SDLC.

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

6.1.3 The FI should ensure its software developers are trained to apply the standards when developing software.

6.1.4 The FI should 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. Where applicable, the FI should include fuzzing or fuzz testing[11] as part of its dynamic or interactive application security testing.

6.1.5 Automated static or dynamic software scanning should be implemented to detect security vulnerabilities or coding issues, and configurations that can impact the security of IT systems. The software scanning rules should be reviewed periodically and kept current.

6.1.6 The FI should ensure issues and software defects discovered from the source code review and application security testing, which affect the confidentiality, integrity and availability of information and the IT system, are tracked and remediated before production deployment.

[10] 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.

[11] Fuzzing or Fuzz testing is an automated software testing technique used to discover coding errors and bugs by inputting random data, known as fuzz, to the system.

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 accommodate business and customer needs. When adopting Agile software development methods, the FI should continue to incorporate the necessary security practices throughout its Agile process to ensure the security of the application is not compromised.

6.2.2 It is important that the FI continue to ensure secure coding, source code review and application security testing standards are applied during Agile software development.

6.3 DevOps Management

6.3.1 DevOps is the practice of automating and integrating IT operations and quality assurance into the software development process to enable frequent, efficient, and reliable releases of software products. The FI should ensure its DevOps 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 enforce segregation of duties for the development, testing and operations functions in its DevOps processes, and ensure the respective DevOps activities are logged and reviewed in a timely manner.

6.4 Application Programming Interface Development

6.4.1 Application programming interfaces (APIs[12]) 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 proprietary software application or web service. FIs collaborate with FinTech companies and develop open APIs, which 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 provision of APIs for secure delivery of such services.

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

6.4.2 To safeguard customer information and the integrity of its systems, the FI should implement strong controls to authorise and control access to designated API services.

6.4.3 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 the third party's nature of business, security policy, industry reputation and track record amongst others.

6.4.4 The FI should perform risk assessment before allowing third parties to connect to its systems via APIs, and ensure the security 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.

6.4.5 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[13], 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.

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

6.4.7 A robust security screening and testing of the API should be performed between the FI and third party before it goes into production. The FI should have the ability to log the access sessions by the third party, such as the identity of the third party making the API connections, and the data being accessed.

6.4.8 Real-time monitoring and alerting capabilities 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.

6.4.9 The FI should implement measures to handle high volumes of API call requests by legitimate applications, and mitigate denial-of-service attacks. The measures to be

[13] 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.

implemented should be commensurate with the criticality and availability requirements of the application.

6.5 Management of End User Computing and Applications

6.5.1 The prevalence of common 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 perform data analysis and generate reports. Any applications developed or acquired by end users should be approved by the relevant business and IT management, and managed as part of the FI's information assets.

6.5.2 The FI should establish a process to assess the importance of end user developed or acquired applications to the business, and ensure appropriate controls and security measures are implemented to address the associated risks. The FI should ensure proper review and testing of the programme codes, scripts and macros before they are deployed and used.

6.5.3 Shadow IT or IT applications acquired and used in the FI's environment without the approval of relevant business and IT management increase the FI's exposure to risks, such as leakage of sensitive data, or malware infection. The FI should establish measures to monitor and detect the use of shadow IT in its environment. End user should not be allowed to use shadow IT until they have been properly assessed and approved for use.

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, 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 system. The FI should implement a configuration management process to maintain and update information of its hardware and software to have visibility and effective control of its systems.

7.2.2 The FI should review and verify the configuration information of its information assets on a regular basis to ensure they are accurate and kept 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 software's end-of-support (EOS) date as service providers may 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 in a timely manner, before they reach EOS should be developed. A risk assessment for hardware and software approaching EOS date should be conducted to evaluate the risks of continued usage and to establish effective risk mitigation controls. The FI should obtain dispensation from its management for the continued use of outdated and unsupported systems.

7.4 Patch Management

7.4.1 A patch management process should be established to ensure 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 to the FI's systems.

7.4.2 All patches should be tested before they are applied to the information assets in the production environment to verify that they do not pose any conflict or compatibility issue with other parts of the affected system.

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 the change implementation. 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 by users before the changes are deployed to the production environment.

7.5.4 A change advisory board, comprising of relevant 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. A system change should be verified after implementation to ascertain if it is working as expected.

7.5.6 Urgent or emergency changes, such as a high priority security patch for a system, are changes that need to be implemented expeditiously and do not 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 the authorisers or approvers for the changes.

7.5.7 Audit and security logs contain useful information which facilitates investigations and trouble-shooting. 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 No single individual should have the ability to develop, compile and move software codes from one environment to another. Strict segregation of duties in the software release process should be practised.

7.6.2 It is important that controls are implemented to maintain clear accountability, traceability and integrity for all software codes that are moved from the non-production environment to the production environment.

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 a system which compromises the confidentiality, integrity and availability of data or systems. The FI should establish an incident management framework with the objective of restoring a disrupted IT service as quickly as possible following an IT incident, to minimise impact to the FI's business and customers.

7.7.2 As part of its incident management framework, the FI should identify and engage the external assistance that it needs to augment its resources to manage IT incidents. This is to ensure sufficient resources are available 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 24/7 incident response capability.

7.7.3 The incident management framework should minimally cover:

(a) the process and procedure for handling IT incidents, including cyber related incidents[14];

(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 systems' performance, availability and security. System events or alerts should be actively monitored so that prompt measures could be taken to address the issues before they lead to an incident.

7.7.5 Relevant stakeholders should be involved in assessing and determining the impact and severity level of an IT incident. The FI should ensure IT incident is escalated and resolved within a timeframe that is commensurate with the severity or prioritisation level of the incident.

7.7.6 The FI should keep its senior management regularly updated on the status of major incidents, such that if there is a need to activate the business continuity or disaster recovery plan, the decision can be made promptly.

7.7.7 The FI should establish a communications plan that covers the process and procedures to apprise its customers of IT incidents that may impede the FI's delivery of financial services to them, and to handle any media or public queries. The FI should identify the spokespersons and subject matter experts to address the media or public queries as well as the platforms to disseminate information.

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

7.7.8 Where necessary, the FI should promptly advise its customers on any actions that may be required on their part. Additionally, the FI should highlight the measures that it is taking to address the IT incident and associated impact to reassure its customers and maintain public confidence.

7.8 Problem Management

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

7.8.2 As a good practice, 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 Availability

8.1.1 Maintaining operational resilience and system availability is crucial in achieving confidence and trust in the FI's operational and functional capabilities. The FI should design and implement its systems to achieve the level of system availability that is commensurate with its business needs. The FI should implement system redundancy or fault-tolerant solutions to achieve the high system availability.

8.1.2 A holistic review of the FI's system and network architectures should be performed to identify any potential single point of failure, and implement appropriate measures to address and mitigate the risk of disruption.

8.1.3 It is particularly important for an FI which operates systems that support real-time transactions to proactively measure and monitor the utilisation of its system and network resources against a set of pre-defined thresholds[15]. Such monitoring could facilitate the FI in carrying out capacity management to ensure IT resources are adequate to meet current and future business needs, or to identify anomalous system or network behaviour for prompt investigation.

8.1.4 To ensure high system availability, procedures to respond to situations when the thresholds defined for IT resources are breached should be established and tested.

8.2 Recoverability

8.2.1 The FI should perform a business impact analysis to determine its business resumption and system recovery priorities in events where an IT incident leads to large scale service disruption. The FI's systems' recovery time objectives (RTO) and recovery point objectives (RPO)[16], should be defined according to its business needs.

[15] 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.

[16] RTO is the duration of time, from the point of disruption, within which a system should be restored. RPO refers to the acceptable amount of data loss for a system should a disaster occur.

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 annually and updated when there are material changes to business operations and information assets.

8.2.3 During the recovery process, the FI should follow the established disaster recovery plan that has been tested and approved by management, and avoid taking untested recovery measures which are likely to carry higher operational risks.

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 plans should comprise:

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

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

8.3.4 If the system and network architectures support load balancing and high availability, the FI should operate from its recovery site for an extended period as part of disaster recovery testing to gain the assurance and confidence that its recovery site is able to support business needs.

8.3.5 Where information assets are managed by service providers, the FI should ensure the disaster recovery arrangements for these information assets are properly tested and

verified to meet its business needs. The FI should participate in the disaster recovery testing that is conducted by service providers managing the FI's critical systems.

8.4 Backup and Recovery

8.4.1 The FI should establish a system and data backup strategy, and develop a plan to perform regular backup so that systems and data can be recovered in the event of a system disruption or when data is corrupted or unintentionally deleted. The backup policy should also address situations where data has been intentionally deleted, corrupted or modified.

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 and processes, 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 restore its system and data backups to validate the effectiveness of its backup restoration procedures.

8.4.4 The FI should ensure any confidential data stored in the backup media is secured (e.g. encrypted). The backup media should be stored 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[17]. In addition, the TVRA should consider the political and economic climate of the country in which the DCs is 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.

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

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

(a) diversification of data communications and network paths by engaging different external service providers;

(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, wet or dry sprinkler systems.

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

8.5.5 The DC's physical security and environmental controls should be monitored on a 24 by 7 basis. Appropriate escalation and response plans and procedures for physical and environmental incidents at data centres 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 immediately if access is no longer required;

(b) proper notification and approval for visitors to the DC. All visitors should be escorted by an 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 recorded, monitored and supervised at all times;

(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', 'segregation of duties', and 'least privilege' should be applied when granting staff access to information assets so that no one person has access to perform critical system functions. Access rights and system privileges should be granted according to the staff's role and job responsibilities.

9.1.2 The FI should establish a user access management process to provision and revoke access rights to information assets. Access rights should be authorised and approved by the information asset owner.

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

9.1.4 The FI should establish a password policy and a process to enforce strong password controls[18] for users' access to IT systems.

9.1.5 Multi-factor authentication[19] should be implemented for users with access to critical system functions[20] to safeguard the systems and information from unauthorised access.

[18] Strong password controls should include a change of password upon first logon, minimum password length and history, password complexity, as well as maximum validity period.

[19] 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.

[20] The criticality of a system function may be assessed based on the sensitivity of the data and criticality of the system.

9.1.6 The FI should ensure 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 incorrectly provisioned access rights. Exceptions noted from the user access review should be resolved as soon as practicable.

9.1.7 The FI should ensure users are granted system access rights on a need-to-use basis. Existing 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 with 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.

9.2.2 System and service accounts are used by the 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 connection 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 hardened 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. 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.

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

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

10.1.4 The FI should monitor development 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 A cryptographic key management policy and procedures covering key generation, distribution, installation, renewal, revocation and expiry should be established.

10.2.2 The FI should ensure cryptographic keys are securely generated and protected from unauthorised disclosure. After a key is generated, the FI should destroy sensitive materials that are used to derive the keys in the key generation process.

10.2.3 The FI should determine the appropriate lifespan of each cryptographic key based on the sensitivity of the data and the criticality of the system to be protected. The cryptographic key should be securely replaced, before it expires at the end of its lifespan.

10.2.4 The FI should ensure the systems that store the cryptographic keys and authenticate customer passwords are hardened and tamper resistant, e.g. hardware security module.

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

10.2.6 If a cryptographic key is found to be compromised, the FI should revoke and replace the key and all other keys encrypted by or derived from the exposed key.

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

10.2.8 When replacing or renewing a cryptographic key, the FI should generate the new key independently from the previous key.

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

11 Operational 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; and

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

11.1.2 The FI should implement appropriate measures to prevent and detect data theft from as well as unauthorised modification in systems and endpoint devices. This should include systems and endpoint devices managed by the FI's service providers.

11.1.3 Databases, 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 databases, systems and endpoint devices should be encrypted and protected by strong access controls.

11.1.4 The FI should ensure only authorised mediums are used to communicate, transfer, or store confidential data. Strong access controls should be implemented to protect the information from unauthorised disclosure.

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 such as social media sites, cloud-based internet storage sites, and web-based emails.

11.1.6 The use of sensitive production data in non-production environment should be prohibited. In exceptional situations where production data needs to be used, proper approval has to be obtained from senior management. The FI should ensure appropriate controls are implemented in non-production environment to manage the access and removal of the data to prevent leakage of confidential data. Where possible, confidential data used in non-production environment should be masked.

11.1.7 The FI should ensure confidential data is irrevocably removed from IT systems and endpoints before they are disposed of.

11.2 Network Security

11.2.1 The FI should install network security devices such as firewalls at critical junctures of its IT infrastructure to secure the FI's connection to untrusted external networks, such as the Internet and connections with third parties.

11.2.2 To minimise the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network, the FI should deploy firewalls, or other similar measures, within internal networks to segregate information assets within the FI's internal networks. Information assets could be grouped into network segments based on the criticality of the business that they support, their functional role (e.g. databases and applications) or the sensitivity of the information.

11.2.3 A security review of the FI's network architecture, including the network design, as well as system and network interconnections, should be conducted on a periodic basis to identify potential security weaknesses. Issues identified from the network architecture review should be tracked and addressed in a timely manner.

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 Network intrusion detection or prevention systems should be deployed at appropriate locations in the network to detect and block malicious network traffic.

11.2.7 Systems with internet access are more susceptible to cyber threats. In this regard, the FI should perform a risk assessment and implement Internet surfing separation by isolating systems, including end-user computers and devices, which handle critical business and system functions or contain sensitive data, from the Internet and other systems connected to the Internet.

11.2.8 If the FI offers online services, an effective Denial of Service (DoS) solution should be implemented to detect and respond to various types of DoS attacks[21]. The FI could engage DoS mitigation service providers to filter potential DoS traffic before it reaches the FI's network infrastructure.

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 include but not limited to behavioural-based and signature-based solutions such as anti-malware should be implemented to protect the FI from malware infection. In particular, the FI should ensure the measures 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 anti-malware signatures are kept up-to-date and the systems are regularly scanned for malicious files or 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 real-time scanning of indicators of compromise (IOCs), and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities.

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.

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

11.3.7 When implementing Bring Your Own Device (BYOD[22]), 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 [23] is used by organisations to optimise the use of computing resources and to enhance resilience. However, several virtual machines that support different business applications can be hosted on a physical system, and a system failure or security breach could have a significant impact on the FI. Hence, the FI should ensure all components[24] of a virtualisation solution have the same level of security and resilience as a non-virtualised IT environment.

11.4.2 The hypervisor and host operating system allow administrative controls over guest operating systems and other components in the virtual environment. Therefore, strong access controls should be implemented to restrict administrative access to the hypervisor and host operating system.

11.4.3 The FI should establish policies and standards to manage virtual machines 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.

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

[23] 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.

[24] 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 are 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, 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 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. The security controls should be commensurate with the function and criticality of the data that is collected, stored and processed by the IoT devices.

11.5.3 The network that hosts IoT devices should be secured using strong authentication and network access controls to limit the cyber attack surface. For instance, restrict the inbound and outbound network traffic to and from an IoT device. The FI may consider hosting 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 manage the administrator access to the IoT devices to minimise the risk of unauthorised access.

11.5.5 The FI should log and monitor the system activities of IoT devices for suspicious or anomalous system activities or user behavioural patterns, particularly outside normal working hours.

12 Cyber Surveillance and 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 could consider procuring cyber intelligence monitoring services, as well as participating in cyber threat information-sharing arrangements with trusted parties.

12.1.3 The FI should use cyber threat intelligence to facilitate its risk assessment on prevailing cyber threats and implement the necessary measures to mitigate the attendant risks.

12.1.4 A process should be established for timely dissemination of cyber related information with internal stakeholders[25] for their awareness or necessary action.

12.1.5 The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services that use technologies, such as machine learning, to facilitate evaluation and identification of online misinformation.

12.2 Cyber Monitoring and Security Operations

12.2.1 The FI should implement monitoring or surveillance systems to ensure it is alerted to any suspicious or malicious system activities[26]. Real-time monitoring of cyber events for critical systems should be performed to facilitate the prompt detection of anomalous activities.

[25] Relevant parties could include CISO, IT security staff, SOCs, risk managers etc.

[26] An example of the abnormal system activities includes multiple sessions using an identical customer account originating from different geographical locations within a short time span.

12.2.2 As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block callbacks, which can be tell-tale signs of intrusions.

12.2.3 A process to collect, consolidate, process and review system logs[27] should be established to facilitate FI's security monitoring operations.

12.2.4 Correlation of multiple events[28] registered on system logs should be performed to identify suspicious or anomalous system activity trend or user behavioural patterns.

12.2.5 Depending on the complexity of the IT environment, the FI should consider implementing tools to perform real-time monitoring and facilitate the analysis and correlation of cyber events.

12.2.6 To facilitate identification of anomalies, the FI should establish a baseline profile of each system and user's routine activity. The profiles should be regularly reviewed and updated.

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

12.2.8 A process should be established to ensure timely response, escalation to relevant stakeholders, and resolution of suspicious or anomalous system activities or user behaviour detected.

12.2.9 The FI should retain its system logs to facilitate investigation of suspicious or unauthorised activities. These logs should be protected against unauthorised access.

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

[28] Examples of event logs are firewall events, authentication events, application events, and operating system events.

12.2.10 To facilitate continuous monitoring and analysis of cyber events; as well as prompt detection and response to cyber incidents, the FI should consider establishing a security operations centre with cyber surveillance and incident response capability.

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 resume affected services as soon as possible. The plan should describe procedures to respond to plausible cyber threat scenarios.

12.3.2 As part of the plan, the FI should establish a process to conduct investigation of a cyber incident to 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 The cyber incident response plan[29] should be reviewed, updated and tested at least annually. Lessons learnt from cyber incidents should be used to enhance the existing controls or improve the cyber incident management plan.

[29] A predetermined set of instructions or procedures to detect, respond to and limit consequences of a cyber incident.

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 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 system and the security risk to which it is exposed.

13.1.2 When performing system VA, the scope should minimally include vulnerability discovery, identification of weak security configurations, as well as applications and services that are not approved by business, IT management and other key stakeholders. For web-based systems, the scope of VA should include checks on common web-based vulnerabilities, such as SQL injection and cross-site scripting.

13.2 Penetration Testing

13.2.1 The FI should carry out penetration testing [30] (PT) 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 mean by which an FI could discover vulnerabilities in their systems by inviting and incentivising ethical or "white hat" hackers to test 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.

[30] 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.

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 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 and review its response and recovery, as well as communication plans against cyber threats. These exercises could include social engineering[31], table-top[32], or cyber range[33] 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.

[31] 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.

[32] 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.

[33] Cyber ranges are interactive, simulated representations of an organisation's local network, 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 is encouraged to perform an adversarial attack simulation exercise[34] 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 do not disrupt the FI's production systems.

13.5 Intelligence-Based Exercise

13.5.1 To simulate realistic adversarial attacks on an FI during a red team exercise, the threat scenario should be designed and based on real cyber incidents.

13.5.2 As an alternative, 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 management 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;
(b) timeframe to remediate issues of different severity; and
(c) risk assessment and mitigation strategies to manage deviations from the framework.

[34] Adversarial attack simulation exercise provides a 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.

14 Online Financial Services

14.1 Security of Online Financial Services

14.1.1 Online financial services refer to banking, trading, insurance, or other financial and payment services that are provisioned via the Internet [35]. In delivering online financial services, the FI should implement security and control measures which commensurate with the risk involved to ensure data confidentiality and integrity, and the security, availability and resilience of the online services.

14.1.2 The FI should secure the communications channel by using strong cryptographic controls to safeguard the confidentiality and integrity of confidential data during transmission such as using 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 [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 risk of mobile applications should be put in place. Refer to Annex C for guidance on Mobile Application Security.

14.1.5 Distribution of mobile applications or software to customers should only be performed through official mobile application stores or other secure delivery channels.

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

[36] 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.

14.1.6 The FI should actively monitor the Internet, mobile application stores, social media websites, emails or text messages (e.g. SMS) for phishing campaigns targeting the FI and its customers. Immediate action should be taken to report the phishing attempts to the service providers and law enforcement agencies to facilitate removal of the malicious content. The FI should alert its customers of such campaigns.

14.1.7 Rooted or jailbroken mobile devices should be blocked from accessing the FI's mobile applications to perform financial transactions as such devices are more susceptible to malware and security vulnerabilities.

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 any two or more of the following factors, i.e. what you know (e.g. personal identification number or password), what you have (e.g. OTP generator) and who you are (e.g. Biometrics).

14.2.2 End-to-end encryption at the application layer 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 system where passwords are verified.

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 apply a risk-based approach and implement appropriate risk-based or adaptive authentication that presents customers with authentication options that commensurate with the risk level of the transaction and sensitivity of the information.

14.2.5 When implementing time-based one-time-passwords (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 information and authentication credentials are encrypted in storage and during transmission.

14.2.7 The performance of the biometrics solution, based on false acceptance rate[38] and false rejection rate[39], should be calibrated to 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]. Where soft token is used for customer authentication, 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 for the soft token provisioning process.

14.2.9 Diversification of cryptographic keys can greatly limit the impact of a key exposure. A unique cryptographic key should be used to generate each type of authentication factors. For instance, the cryptographic key for generating the OTP for login should be different from the one that is used to generate the transaction-signing code.

14.2.10 A process should be implemented to secure the issuance and enrolment of the authentication or transaction signing mechanism so as to prevent the theft of the mechanism for unauthorised access to the FI's customer's online account.

[37] Biometric recognition technologies could be based on face, iris or palms image, 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] Such as 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.

14.2.11 The FI should ensure the authenticated session, together with its encryption protocol, remains intact throughout the interaction with the customer. In the event of interference, the FI should put in place measures to detect and terminate the session. To prevent an attacker from maintaining a hijacked session indefinitely, online session should be automatically terminated after a pre-defined time.

14.2.12 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 to ascertain these controls or processes commensurate with the risk of the activities that are being carried out.

14.3 Fraud Monitoring

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

14.3.2 A follow-up process should be established to ensure suspicious transactions or payments are investigated and issues are adequately and promptly addressed.

14.3.3 The FI should notify customers of suspicious activities or fund transfers above a threshold that is defined by the FI or customers to facilitate detection and response to fraudulent transactions in a timely manner. 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 about the risks of using online financial services before they subscribe to such services and whenever changes are made to the security features of the services.

14.4.2 The FI should advise their customers on the means to report security issues, suspicious activities or fraud.

[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).

14.4.3 The FI should alert their customers to cyber threats and incidents, and educate their customers of their responsibilities to take appropriate security measures to secure the electronic devices that are used to access online financial services.

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 risk.

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 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 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 a system in its run-time state. The tester has 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 a system.

Annex B: BYOD Security

B.1 The FI should implement data loss prevention measures on personal 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 management and virtualisation solutions. These solutions can be augmented with other security measures for mobile devices to provide enhanced functionalities:

(a) Mobile Device Management

Mobile Device Management (MDM) solutions are used to manage and control mobile devices used to access the FI's resources. Before a mobile device is permitted to access the FI's network, the device is verified to ensure it has not been "jailbroken", "rooted" or compromised. MDM solutions usually come with storage encryption, "lock and wipe" capabilities and can be used in conjunction with other security measures. A robust MDM solution should be implemented for all BYOD arrangements.

(b) Virtualisation

Virtualisation allows staff to have on-demand access to enterprise computing resources and data from their mobile devices using strong authentication and network encryption. The FI's data is not downloaded into the mobile device as it is processed within the corporate data centre. Strict security policies should be enabled within the virtual environment to restrict copying and use of peripheral devices, such as printers, 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 follow:

(a) avoid storing or caching data in the mobile application to mitigate compromise of the data on the device;

(b) 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;

(c) 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;

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

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

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

Monetary Authority of Singapore