GUIDELINES TO FINANCIAL INSTITUTIONS

GUIDELINES NO. TRS/G-2/2022/1

GUIDELINES ON
TECHNOLOGY RISK MANAGEMENT (TRMG)

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Information Technology (IT) has transformed the way financial institutions' businesses and operations are being conducted and become key enablers for business strategies of the Financial institutions (FIs). FIs are providing more advanced as well as innovative products and services to keep pace with the needs and preferences of consumers who are becoming more tech-savvy.

1.2 As such, FIs need to fully understand the degree and level of technology risk from these IT transformation and digital financial services by putting in place adequate and robust risk management systems as well as control processes to manage these risks.

1.3 These Guidelines on Information Technology Risk Management aim to provide guidance to FIs in managing risks associated with the use of IT and digital financial services based on industry best practices and internationally recognised standards.

1.4 The objectives of these Guidelines are to:

i. Encourage FIs to establish a sound and robust information technology risk management framework;

ii. Promote effective IT governance and IT management on the FIs;

iii. Strengthen FIs' system security, reliability, resiliency and recoverability; and

iv. Deploy strong IT controls to protect customer data, transactions and systems.

1.5 The Guidelines are issued pursuant to section 32 of the Brunei Darussalam Central Bank Order, 2010 and are aimed at FIs licensed, registered or regulated under any of the following legislations:

i. Banking Order, 2006;

ii. Islamic Banking Order, 2008;

iii. Insurance Order, 2006;

iv. Takaful Order, 2008;

v. Finance Companies Act, Cap. 89; and

vi. Securities Markets Order, 2013.

1.6 These Guidelines are also applicable to:

i. operators of payment systems that have been approved to operate in Brunei Darussalam under the Notice on Requirements for Payment Systems (Notice No. PSO/N-1/2020/1); and

ii. Perbadanan Tabung Amanah Islam Brunei established under the Perbadanan Tabung Amanah Islam Brunei Act (Cap. 163).

1.7 These Guidelines should be read with the following:

i. Notice on Application for Approval of Outsourcing Arrangement for Insurance Companies and Takaful Operators (Notice No. TIU/N-1/2019/11);

ii. Notice on Early Detection of Cyber Intrusion and Incident Reporting (Notice No. FTU/N-1/2017/1 and TRS/N-1/2020/1];

iii. Notice on Market Conduct (Notice No. FCI/N2/2021/1);

iv. Notice on Outsourcing for Capital Markets Services Licence Holders (Notice No. CMA/N-1/2020/15);

v. Notice on Requirements for Payment Systems (Notice No. PSO/N-1/2020/1);

vi. Notice for the Establishment of a Complaints Handling Function within Financial Institutions (Notice No. FCI/N1/2021/1);

vii. FinTech Regulatory Sandbox Guidelines (Guideline No. FTU/G-1/2017/1);

viii. Guidelines on IT Third Party Risk Management (TRS/G-3/2022/2);

ix. Guidelines on Online Distribution for Insurance Companies and Takaful Operators (Guideline No. TIU/G-1/2020/11);

x. Guidelines on Outsourcing Arrangement for Insurance Companies and Takaful Operators (Guideline No. TIU/G-1/2019/10); and

xi. Guidelines on Outsourcing for Banks.

1.8 Implementation of these Guidelines should be risk-based and commensurate with the size of the FIs' business, nature and types of products and services offered by the FIs, as well as the complexity of the FIs' IT operations.

1.9 These Guidelines shall take effect on 1st July 2022 and shall supersede the Guidelines on Information Technology Risk Management (Guideline No. BS/G-1/2015/4) which is hereby repealed.

2. DEFINITIONS

For the purpose of these Guidelines:

2.1 "Acceptable usage policy" refers to policy that define how to properly use IT resources in the FIs including restrictions.

2.2 "Active-active pairing" refers to when both devices are actively transmitting and receiving data.

2.3 "Application Programming Interface" or "API" refers to software intermediary or a set of programming codes that enables data transmission or add-on functionality between one software to another software.

2.4 "Artificial intelligence" refers to software that provide automation capability for computer or machine to perform tasks that are normally performed by humans.

2.5 "Audit trail" refers to series of records of computer events such as for an operating system, an application, or user activities.

2.6 "Automated Teller Machine" or "ATM" refers to a machine that allows customers to perform cash transactions or to obtain information without the need to go to the bank and deal with a teller. Some of the uses of ATMs include cash withdrawals, bill payments, printing bank statements, etc.

2.7 "Behaviour analytics" refer to the use of software to analyse the activities and actions performed by a user to predict the user's behaviour.

2.8 "Business Continuity Management" or "BCM" refers to management process that identifies risks, threats and vulnerabilities that could impact a FIs' continued operations. BCM also provides a framework for building organizational resilience and the capability for an effective response.

2.9 "Bring Your Own Device" or "BYOD" refers to devices that personnel brings to the office to carry out tasks but are not assets provided by the FIs or service provider e.g. personal handheld devices, personal laptops, desktops, etc.

2.10 "Cache" or "caching" refers to reserved storage location that collects temporary data to assist websites, browsers and apps load faster.

2.11 "Capacity Management" refers to process in ensuring technical capacity of IT services and infrastructure is able to deliver agreed performance targets efficiently in a cost effective and timely manner.

2.12 "Card-not-present" refers to when information about a cardholder's payment card e.g. account number and expiry date, is used to make purchases over email, phone or internet (where the presence of the physical card is not required).

2.13 "Card-not-received" refers to a situation when a payment card dispatched to the cardholders by issuing banks are intercepted and used to make fraudulent transactions.

2.14 "Cash Deposit Machine" or "CDM" refers to a machine that allows customers to perform cash deposit without the need to go to the bank and deal with a teller. Several uses of CDMs include cash deposit, top ups and bill payment.

2.15 "Certificate based digital signature" refers to the use of an encryption key file called a certificate to provide the highest level of assurance of the signer's identity.

2.16 "Change Management" refers to the process of planning, coordinating, implementing and monitoring changes affecting any IT systems.

2.17 "Chatbot" refers to computer program designed to simulate human conversation. The chatbot provide words given to them by a person and provide pre-set answers.

2.18 "Chief Information Security Officer" or "CISO" refers to senior officer in a FIs whose main role is focused on information security issues.

2.19 "Chief Information Officer" or "CIO" refers to a senior officer in a FIs whose main role is focused on IT strategy as well as overseeing the IT services and operations.

2.20 "Cloud Computing" refers to service and delivery model for enabling on-demand network access to a shared pool of configurable computing resources (servers, storage and services). Hosting, storing or processing of information are within the service provider's computing infrastructure.

2.21 "Coin Deposit Machine" or "CoinDep" refers to a machine that allows customers to perform coin deposit without the need to go to the bank and deal with a teller.

2.22 "Common workstation" refers to shared desktop computer within office space used for common office purpose such as scanning document, printing or Internet access. This exclude workstation shared between system users (e.g. front-line counter, helpdesk or call centre), which should have other controls in place commensurate with the risks.

2.23 "Compromise assessment" refers to the expert analysis of logs, events and reports on the system, server, network and end-user focusing on identifying if there are any traces of successful cyber intrusions or attacks on the system.

2.24 "Consultant" refers to an external individual or entity that provides expert advice and technical assistance to the FIs in IT related matters.

2.25 "Contractors" refers to vendors, suppliers, service providers, outsourced service providers and/or consultants that have made contract with the FIs to provide specific and consistent products or services to the FIs. Contractors are usually effective during IT project or within time period of the agreed contract.

2.26 "Counterfeit" refers to when a payment card data is transferred onto a fake magnetic stripe card through skimming method or simply using information on account number and expiration.

2.27 “Critical system” refers to any system that supports the provision of FIs services, where failure of the system can significantly impair the FIs’ provision of services to its customers or stakeholders, business operations, financial position, reputation or compliance with applicable laws and regulatory requirements.

2.28 “Cybersecurity” refers to the practice of securing technology in order to protect confidentiality, integrity and availability of FIs’ system and data in the digital space.

2.29 “Demilitarised Zone” or “DMZ” refers to perimeter network or subnetwork that sits between the public internet and private network.

2.30 “DevOps” refers to software development methodology that combines software development and IT operations, and emphasis continuous improvement.

2.31 “DevSecOps” refers to the integration of security practices into DevOps methodology.

2.32 “Disaster Recovery Plan” refers to plan that covers the tactical recovery of IT systems in the event of a disruption or disaster.

2.33 “Electronic Wallet” or “e-Wallet” refers to applications or prepaid facilities (i.e. prepaid card, virtual card) that stores monetary value, or is linked to credit/debit cards and bank account.

2.34 "End-of-Support” or “EOS” refers to when a product has ceased to be available from the market and vendor support is no longer available.

2.35 “End-user” refers to individual or personnel that uses FIs’ IT system and IT assets for their business operations and activities.

2.36 “Encryption” refers to the process of encoding messages or information in such a way that only authorized parties can read it.

2.37 “Europay, Mastercard and Visa” or “EMV” cards refers to open standard set of specifications for smart card payments and acceptance devices. EMV cards are smart cards that store their data on integrated circuits rather than magnetic stripes. These cards are also known as chip and PIN cards.

2.38 “Error rate” refers to the percentage of instances when an AI system produces result that is not according to the predefined rules or algorithm intended by the developer (e.g. false result, wrong action executed, no output). Error rates are evaluated based on the following:

$$\text{Error rate} = \frac{No.\ of\ \text{Error Result}}{(No.\ of\ \text{Error Result} + No.\ of\ \text{Correct Result})} \times 100$$

2.39 “False positive alerts” refers to alerts wrongly generated by AI system or alerts that do not match the predefined alert rules.

2.40 “Firewall” refers to device or program that control the flow of network traffic between networks or hosts by provisioning rules and filters to protect FIs from malicious network traffic.

2.41 "High availability" refers to characteristic of IT system designed to avoid loss of service by reducing or managing failures and minimising planned downtime.

2.42 "Homogenous data structure" refers to grouping or storing of data into similar data types such as using tables to group similar data in a database.

2.43 "Host virtual machine" refers to the main "machine" or server that manage all other virtual servers.

2.44 "Identity Theft" refers to when criminal obtains sensitive information of an individual or entity to conduct social engineering attack such as account takeover or transaction fraud.

2.45 "Incident Management" refers to the process of managing the lifecycle of incidents and to restore the service as quickly as possible.

2.46 "Information Security" refers to the practice of protecting information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security cover both physical and digital information.

2.47 "Information Technology Steering Committee" or "ITSC" refers to committee consisting of senior members of the FIs' management that determines the prioritization of IT projects, and tracks and monitors the status of IT projects. The committee resolves any arising conflicts as well as monitoring service levels and service improvements.

2.48 "Internet Banking" refers to an electronic system that enables customers of a FIs to perform banking activities online on a website operated by the FIs.

2.49 "Intrusion Detection" refers to the process of identifying attempts to penetrate a system and gain unauthorized access.

2.50 "IT Audit" refers to formal inspection and verification to check whether IT standards, policies and guidelines are being followed by the FIs' personnel including in implementing IT controls and ensuring target efficiency and effectiveness of IT systems and operations are being met.

2.51 "IT Consumables" refers to removable hardware extensions, attachments and/or accessories that can be connected or inserted into an IT asset such as USB drives, headphones and external webcam. However, it does not include disposable consumables such as paper, ink and CDs.

2.52 "IT Operations" refers to the people and management processes associated with IT service management to deliver the right set of services at the right quality and at competitive costs for customers.

2.53 "Kiosk" is a terminal or machine that is used to provide information and perform query on non-payment service. Kiosk in general, covers machine that are not covered under MFM.

2.54 "Major IT application" refers to IT application that is used for critical business operations, delivery of FIs' core services and handling of customer's personal data.

2.55 "Major IT incident" refers to an IT incident which has a severe and widespread impact on an FI's operations and service delivery, or has a material impact to an FI.

2.56 "Maker-Checker control" refers to authorisation principle where for any application or transaction, there must be at least two individuals necessary to process the application or transaction.

2.57 "Manufacturer" refers to individual or entity that prepares finished products for sale and distribution.

2.58 "Media degaussing" refers to the process or technique of destroying data in a hard disk drive using strong magnetic field.

2.59 "Mobile Banking" refers to electronic system that enable customers of a FIs to conduct banking activities through mobile phone devices.

2.60 "Multifactor authentication" or "two-factor authentication" refers to combining one or two forms of authentication method based on different factors: knowledge (e.g. password, PIN), possession (e.g. SMS one-time PIN, soft token, device binding), biometric (e.g. Face ID, fingerprint), behavioural (e.g. user activity) and location (e.g. location service, IP address)

2.61 "Multi-function Machine" or "MFM" refers to a machine that allows FIs to provide branchless service to the customer such as cash withdrawal, cash deposit or cheque deposit.

2.62 "Negative consent method" refers to a method to request consent in which the FIs can assume customer's consent if the customer does not provide response after a given period of time.

2.63 "Online payment gateway" or "payment gateway" refers to online payment service that, when integrated with e-commerce platform, is devised as the channel to make and receive payments. The online payment gateway is mainly to approve transaction between merchant and customer.

2.64 "Open API" refers to publicly available API that provides a developer with programmatic access to a certain feature of the FIs' application or service.

2.65 "Open source software" refers to software that is released with its source code available to the public. This allows the software to be inspected, modified and enhanced. The software is usually developed by community group, sometimes at no fee.

2.66 "Off--the-shelves software" refers to commercial software that is already in a finished state and ready for distribution.

2.67 "Payment card" refers to ATM/debit/credit/prepaid cards that can be used by customers of FIs to make a payment at Point of Sales (POS) or other payment devices. Payment cards typically contain a magnetic stripe or a chip that contains unique information that belongs to the cardholder.

2.68 "Penetration testing" or "PenTest" refers to testing by means of an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.

2.69 “Personal Identification Number” or “PIN” refers to numeric password shared between a user and a system that can be used to authenticate the user to the system.

2.70 “Personal data” refers to data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the FI has or is likely to have access.

2.71 “Phishing” refers to the attempt to acquire sensitive information such as usernames, passwords, and debit/credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity via an electronic communication.

2.72 “Problem Management” refers to process to find a permanent solution to a problem or recurring incident.

2.73 “Project” refers to a temporary endeavour undertaken to create unique product or service. It has defined scope and consists of sets of operations to deliver specific goal.

2.74 “Project Management” refers to process and activity of planning, organising, motivating, controlling resources, procedures and protocols to achieve specific goals in a project.

2.75 “Private API” refers to API that is limited for FIs’ internal system or for third party system in which the FIs and the third party has made prior formal agreement.

2.76 “Pseudonymisation” refers to data management process in which personal information within a data records or fields are replaced with unique identifiers (e.g. URN).

2.77 “QR code” refers to machine-readable code that can instantly be read using a smartphone camera or device, that typically used for storing URLs or bank account details.

2.78 “Recovery Point Objective” or “RPO” refers to the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure.

2.79 “Recovery Time Objective” or “RTO” refers to the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels.

2.80 “Remote Desktop Protocol” or “RDP” refers to an operating system protocol that allows a user to remotely connect to a machine from another machine.

2.81 “Risk appetite” refers to the level of exposure that an organisation is willing and prepared to accept. Risk appetite for each IT asset and system should be agreed at Board level and properly documented.

2.82 “Risk register” refers to a risk profile report of the risks identified by the FIs, quantification where relevant, and the extent to which the risks have been managed and mitigated. The register should also include the interdependencies, wherever relevant, should be identified so that decisions on risk management are not taken in isolation.

2.83 "Robo-Advisory" refers to a digital platform that provides advice, recommendation or alternative suggestion for the customer to make decision on the types of financial product or services suitable for them without the needs to interact with FIs' human representative.

2.84 "Sandbox" refers to creating isolated environment in an IT system or operating system so that any changes in the environment will not affect the main environment.

2.85 "Secure Socket Layer" or "SSL" refers to cryptographic protocol that uses explicit connections to establish a secure communication between web server and client.

2.86 "Security Information and Event Management" or "SIEM" refers to software tool that provides a holistic view of an organisation's security events and logs.

2.87 "Security Operations Centre" or "SOC" refers to centralised function for information security monitoring and analysis in order to understand the FIs' cybersecurity posture and respond to cybersecurity incident.

2.88 "Senior Management" refers to upper management or executive management of the FIs, which is the highest level of management that are responsible to carry out direction from the board of directors and lead the organisation.

2.89 "Senior Officer" refers to personnel from the FI that report directly to Senior Management or Country Manager of FI.

2.90 "Service provider" refers to an individual or entity that provides a service to the FIs, including a member of the group to which the FIs belongs, e.g. its Head Office, parent insurer, another branch or related company, whether it is located in Brunei Darussalam or elsewhere.

2.91 "Software-as-a-Service" or "SaaS" refers to cloud delivery model where cloud service provider hosts an application, while the client can access the application via the internet.

2.92 "SDLC" or "Software Development Lifecycle" refers to methodology with clearly defined processes for developing software, in which every phase of the SDLC has its own process and deliverables.

2.93 "Source Code" refers to text listing of commands or instructions written using some human-readable computer language, usually as text.

2.94 "Supplier" refers to external individual or entity that provide and distribute IT products including hardware and software to the FIs.

2.95 "System" refers to information system used by the FIs for performing their business operation, which is made up of hardware, software, network, and other IT components.

2.96 "System acquisition" refers to the process of acquiring IT system for the FIs, through purchase or development.

2.97 "System development" refers to the process of developing software or application from scratch or based on minimal templates in order to better suit the FIs' requirements. This should be performed by the FIs' IT team (in-house) or by a third party (outsourced).

2.98 “System owner” refers to business unit that owns and manages the operation of specific IT application or system in the FIs. This is mainly because the application or system involves business process and data of the business unit.

2.99 “Technology risk” refers to any risks that is caused by IT and IT-related failure or vulnerability, which can impact FIs’ systems, data and business processes.

2.100 “Third party system” refers to IT system or application that is owned and managed by a third party or external stakeholders, with the exception of government agencies and regulators.

2.101 “Threat” refers to act or agent that can exploit vulnerability in FIs’ business operation or IT environment.

2.102 “Three line of defence” refers to governance model that provides effective way to enhance communications of risk management and control in the FIs by clarifying essential roles and duties into three lines: operational management, risk and compliance, and assurance or internal audit.

2.103 “Transport Layer Security” or “TLS” refers to cryptographic protocol that provides end-to-end security of data sent between applications over the internet.

2.104 “Vendor” refers to external individual or entity that offer solutions to FIs directly or through suppliers and service providers. Vendor usually liaise on the business relationship with the FIs and engaged with suppliers and service providers to deliver products or services.

2.105 “Virtual machine” or “VM” refers to technology that allow FIs to use one physical machine to host multiple “machines” or “servers”.

2.106 “Virtual private network” refers to secure private network or protocol that authenticate, encrypt and transmit data between two points in a network or the Internet.

2.107 “Virtual server” refers to the individual “servers” inside a virtual machine.

2.108 “Vulnerability” refers to weakness in business operation, process, IT asset, IT system and people that can be exploited or exacerbate by threat.

2.109 “Vulnerability assessment” or “VA” refers to the process of detecting and identifying security vulnerabilities in a system through security assessment, in order to prioritise resolutions and patching activities.

3. IT GOVERNANCE

Considering that technology has become a major part in supporting business operations and service delivery in FIs, the Board of Directors ("Board") should therefore ensure their FIs establish an effective IT governance framework that covers leadership and organizational structures. IT governance should cover the following processes:

i. Aligning IT strategic plan with the FIs' overall business strategy;
ii. Optimisation of resources management;
iii. Effective and efficient use of technology to achieve business objectives and performance; and
iv. Ensuring IT considerations on the three lines of defence of the organisation.

3.1 Framework and Strategy

3.1.1 The Board should ensure Senior Management establishes a suitable technology risk management framework for the FIs.

3.1.2 FIs should review and perform gap analysis on their IT and cybersecurity environment based on applicable law or regulation, and internationally recognised framework or standards.

3.1.3 FIs should also establish indicator based on the framework to help the FIs to evaluate their IT management maturity level and set their desired maturity level commensurate with the size, nature and types of products and services as well as the complexity of IT operations of the FIs.

3.1.4 The Board should have sound understanding of the IT Strategy of the FIs and ensure the Senior Management has established strategic actions plans that are aligned with the FIs' business strategy and the approved technology management framework.

3.1.5 Senior Management should be involved in key IT decisions that may affect the FIs' business strategy and ensure the Board are made aware of the decisions

3.1.6 The Board should ensure the Senior Management has assigned adequate resources and expertise to implement and enforce the IT strategy.

3.1.7 Senior Management should ensure that the FIs has the necessary expertise and resources prior to introducing new product or services or to adopt new technologies on the FIs.

3.1.8 Senior Management should conduct periodic review of their technology management framework and IT strategy so that it is commensurate with the usage of technology in the FIs.

3.1.9 The IT strategy should also be communicated to other business functions in the FIs to allow the respective business functions to align their technology expectation and adoption with the IT strategy.

3.1.10 For FIs that are incorporated outside Brunei, the role of the Board can be undertaken by its group/regional or its equivalent oversight function that oversee operations and Senior Management in Brunei.

3.2 Organisational Structure

3.2.1 FIs should designate a Chief Information Officer (CIO), or equivalent, responsible to lead the IT management of their organisation, which include the following job scope but are not limited to:

i. IT project and third-party management;
ii. IT service management including change and incident management;
iii. management of day-to-day technology operations;
iv. keep apprised of current and emerging technology; and
v. monitoring and maintaining performance of the system;

3.2.2 For FIs incorporated outside Brunei, the FIs should designate a senior officer at the local office to keep well-informed with any technology initiatives from the Group CIO.

3.2.3 The FIs should also designate a Chief Information Security Officer (CISO) or equivalent, who are not the CIO or equivalent. The CISO should be responsible for the management of information security and cybersecurity, which include the following job scope but are not limited to:

i. management of information security program;
ii. handling of cybersecurity operations and services;
iii. keep apprised of current and emerging cyber risk, threat and incident;
iv. management of cybersecurity incident;
v. review information security architecture; and
vi. developing and coordinating information security awareness campaigns.

3.2.4 For FIs incorporated outside Brunei, the FIs should designate a senior officer at the local office to keep well-informed with any information security initiatives from the Group CISO or equivalent.

3.2.5 The FIs should ensure that the CIO and CISO has sufficient authority and resources to effectively performed their role.

3.2.6 The CIO and CISO should establish roles and responsibilities for their IT personnel and cybersecurity personnel respectively. The roles and responsibilities should be clearly defined, communicated to the aforementioned personnel and properly documented.

3.3 Oversight and Reporting

3.3.1 The Board should ensure the Senior Management have adequate oversight on technology risks management and ensure their FIs implemented internal controls and maintained their risk management practices. The Board and Senior Management will be responsible and accountable for any important IT decision and operations in the FIs.

3.3.2 The Board and/or Senior Management should have at least a member that is well informed of technology risks relating to their FIs, which include risks posed by technology failures and cyber threats.

3.3.3 The Board should establish or designate a management level committee (herein will be referred to IT Steering Committee or ITSC) for effective and efficient IT related decision-making process. The ITSC should report to the Board, board-level committee such as the Risk Management Committee or equivalent, or the Senior Management subject to the FIs' size and structure.

3.3.4 The ITSC should oversee information technology related strategies and projects as well as monitoring them to ensure they effectively support the FI's business needs and objectives. The ITSC should also become a platform to escalate and discuss any IT matters that require major decision making.

3.3.5 The ITSC should convene a meeting at least on a half yearly basis and the minutes of meeting should be properly documented and distributed.

3.3.6 At a minimum, the ITSC should consist of the following:

i. A member of Senior Management;
ii. CIO or the Head of IT function;
iii. CISO or the Head of Information Security function;
iv. Senior officer who oversees business operations;
v. Senior officer who oversees digital financial services; and
vi. The Head of Risk Management and Compliance in advisory capacity only.

3.3.7 If the ITSC do not report directly to the Board, the Board or Senior Management should identify a board-level committee for regular reporting of technology related matters and establish reporting line on technology oversight through the board-level committee.

3.4 IT Policies, Standard, Guidelines and Procedures

3.4.1 FIs should establish IT policies based on board-approved framework, strategy and/or corporate policy. These policies should be aligned with the overall business objectives and IT strategies of the FIs.

3.4.2 IT policies should be adapted based on applicable national and international laws, regulations and code of practices, as well as relevant IT standards and financial industry's best practices.

3.4.3 Depending on the scope and complexity of some IT policies, FI should also establish standards and guidelines to support implementation of the IT policies.

3.4.4 Policies, standards and guidelines should be reviewed regularly to accommodate ever-changing technology and cybersecurity environment. The Senior Management should ensure that these policies, standards, and guidelines are up to date and well documented.

3.4.5 Policies, standards, and guidelines should be clearly communicated and made available for access to all personnel.

3.4.6 In terms of procedure, FIs should document standard operating procedures and manuals to understand the IT processes and business operations of digital financial services. The procedures should also be communicated and made available for access to the relevant personnel.

3.4.7 Procedures should also be reviewed regularly to accommodate the change in IT environment and FIs' business operations, as well as to reflect updates in policies, standards and guidelines where applicable.

3.5 Risk Management

3.5.1 The Board should ensure that Senior Management maintains a sound risk management program for oversight of technology risk management and proper execution of risk management and security controls processes. It is recommended to establish a risk management function or officer to develop and facilitate the risk management program for the FIs.

3.5.2 The program should include the following attributes:

i. Clearly defined and documented roles and responsibilities of relevant stakeholders in managing technology risks; and

ii. Systematic and consistent procedures in place for technology risk identification, assessment, responses and monitoring.

3.5.3 Risk Identification

i. The FIs should identify vulnerabilities in relation to their business operations and IT environment such as by conducting gap analysis and security assessment; and

ii. The FIs should identify threats that can exploit or exacerbate the vulnerabilities relating to their business operations and IT environment.

3.5.4 Risk Assessment

i. A set of criteria measuring and determining the likelihood and impact of threats and vulnerabilities should be established. The FIs should take into consideration of financial, operational, legal, reputational and regulatory factors in assessing technology risks.

ii. The Board and Senior Management should also set a suitable risk appetite for the type and extent of technology risks the FIs is willing and able to assume;

iii. FIs should establish prioritisation by identifying risks that have the highest exposure to loss and/or severity level of damage; and

iv. The outcomes of the risk assessment should be communicated to Senior Management and the Board.

3.5.5 Risk Response

i. For each type of risk identified, the FIs 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.

ii. The FIs should also assess its risk tolerance for damages and losses in the event that a given risk-related event materialises, in line with the risk appetite of the FIs.

iii. As it may not be practical to address all known risks simultaneously or in the same timeframe, the FIs should give priority to threats and vulnerabilities with a higher risk rating.

iv. In addition, FIs should address threats and vulnerabilities with medium or low risk rating based on suitable timeline commensurate to the impact.

v. The FIs 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 FIs should assess the effectiveness of the controls and security measures with regard to the risks being mitigated.

vi. The FIs should refrain from implementing or acquiring IT system where threats to the safety and soundness of the FIs cannot be adequately controlled and the risks out-weigh the benefits.

vii. As there are residual risks from threats and vulnerabilities which cannot be fully eliminated, the FIs 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 be commensurate with the FIs' risk tolerance. Acceptable or residual risks should be formally endorsed by the Senior Management and monitored.

viii. IT control and risk mitigation approach should be subjected to regular review and update, considering changes in threat landscape and variations in the FIs' risk profile.

3.5.6 Risk Monitoring

i. Continuous monitoring is important to ensure that the risk processes are effective, to identify risk impacting changes to the FIs' IT systems and the environments in which the systems operate, and to verify that all of these risk responses are implemented and communicated within the FIs.

ii. 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 and Senior Management. The frequency of monitoring and reporting should be commensurate with the level of risk.

iii. 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 FIs should consider risk events and audit observations, as well as refer to regulatory requirements.

3.5.7 The Senior Management should be involved in key IT decisions that may change the FIs' risk appetite and any major change should be approved by the Board.

3.6 IT Compliance

3.6.1 In addition to laws and regulations, FIs should implement or determine a second line of defence function to assess and verify that IT policies, standards, guidelines and procedures are being adhered by the FIs' personnel.

3.6.2 The second line of defence should include follow-up processes to ensure compliance deviations are identified, monitored, addressed and remediated in a timely manner.

3.6.3 FIs should clearly define the consequences of non-compliance with their policies and standards.

3.6.4 The FIs should ensure the integrity of the process or system used to manage and prove their IT systems are complying to policies and standards.

3.7 Internal Audit

3.7.1 Internal Audit plays an important role to assess the effectiveness of the controls, risk management and governance process in the FIs. The FIs should ensure IT audit is performed or to include IT into their overall audit. This is to provide the Board and Senior Management an independent assurance of the adequacy and effectiveness of the FIs' IT risk management, governance and internal controls relative to its existing and emerging technology risk.

3.7.2 During audit planning, the Internal Audit should perform effective risk-based assessment on the FIs' strategic plans, business objectives and regulatory requirements. The risk assessment should also consider the risks identified from the FIs' technology risk management framework.

3.7.3 The scope of IT audit may cover the following auditable areas:

i. IT Governance;
ii. IT System and Project;
iii. IT Infrastructure and Operations;
iv. IT Services and End-Users;
v. IT Security;
vi. IT Incident and Business Continuity Management;
vii. Digital Financial Services; and
viii. Consumer Protection.

3.7.4 The scope of the IT audit and list of auditable activities should be documented clearly in the IT audit plan. The IT audit plan should be reviewed and approved by the Audit Committee or equivalent board-level committee before an audit is initiated.

3.7.5 FIs should establish an IT audit cycle of at least once a year or at a frequency to be determined and endorsed by the FIs' audit committee based on their internal audit methodology and commensurate to the risks relating to the IT systems and operations.

3.7.6 The FIs should ensure IT audit findings or issues are addressed within a reasonable timeframe by the relevant business units. The IT auditors should evaluate proposed action items, justifications and/or compensating controls submitted by the business units.

3.7.7 IT audit report should be communicated to the Board and Senior Management, to help them better understand and support the audit recommendations as well as clarify any issues and business concerns.

3.7.8 Consequently, a follow-up process to track and monitor IT audit issues, as well as an escalation process to notify the relevant IT audit issues to the Senior Management and relevant stakeholders, should be established.

3.7.9 The FIs should ensure its IT auditors (internal and/or external) have the requisite level of competency and skills to effectively assess and evaluate the adequacy of IT policies, procedures, processes and controls implemented.

3.8 Role of Business Units

3.8.1 Business units can be a system owner, end-user of the system, or both. Therefore, the business units should understand their part in ensuring security of their system, such as adhering to policies, standards and guidelines and ensuring IT controls in the system are maintained.

3.8.2 The FIs should ensure the business units have a sufficient procedure and manual as well as awareness on the safe and acceptable use of IT and system, tailored to the role of the business unit.

3.8.3 Since the business units are more familiar with their functions and business operations, the business units should also be involved in the preparing the FIs' technology risk management and reporting of risks relating to their business operations.

3.8.4 The head of business units should ensure there are segregation of duties being practiced, such as by implementing Maker-Checker control in critical processes or activities on the FIs' IT system and operations.

3.9 Personnel Selection Process

3.9.1 In order to minimise internal threats in the FIs, a background check and security screening process in the selection of new FI's personnel is crucial. This include but not limited to the following:

i. Financial status;

ii. Sanctioned list;

iii. Criminal record;

iv. Previous and current employer(s); and

v. Directorship, partner, subsidiary and affiliates.

3.9.2 Competency assessment should also be carried out in the selection of personnel. This can reduce risk relating to human error, carelessness and lack of expertise when handling technology and IT operations.

3.9.3 FI's personnel who are authorised to access the FIs' systems and sensitive data should be required to protect sensitive and confidential information. FIs should request that they sign a non-disclosure agreement to ensure information security.

3.9.4 FIs should also have resource and succession planning to ensure continuity of business operation in the event of unforeseen circumstance such as job shadowing, job rotation and backup personnel.

3.10 Competency Management

3.10.1 With the rapid development in technology, FIs should ensure that their IT personnel remain competent and are up to date with the latest advancement in technology, cyber threats and IT risks through training or certification.

3.10.2 FIs should also have strategic human capacity planning for IT operations and processes to identify current and future human resource needs. Appropriate recruitment, succession and transition strategies should be put in place to avoid workforce shortages or spares that could affect the effectiveness, efficiency and productivity of the FIs' IT and business operations.

3.10.3 FIs should ensure that their IT personnel have relevant skills and qualifications to undertake their specific roles. As certain software and hardware may require specialised skill, FIs should have at least one personnel to be familiar or equipped with specific knowledge on the software and hardware used by the FIs.

3.10.4 FIs should also establish information sharing and/or knowledge transfer program between related IT personnel to ensure smooth job handover process in the event that the main personnel become unavailable such as termination of contract or emergency leave.

3.11 IT Awareness

3.11.1 A comprehensive IT and information security training and awareness program should be established to enhance the overall IT and information security awareness level in the FIs. The training and awareness program should be conducted on a regular basis.

3.11.2 The FI should also provide its board members with relevant training and information on technology developments periodically to enable the board to effectively perform its oversight role.

3.11.3 The FIs should assess the IT security awareness level of their personnel periodically to evaluate the effectiveness of the IT security training and awareness program.

3.11.4 FIs should consider the following when planning IT and information security training and awareness program in their organisation:

i. Ensure that all personnel and users of their information systems are made aware of the features on their information system and are adequately trained to carry out their duties and responsibilities using the information systems.

ii. Ensure that all personnel and users of their information systems are made aware of the security risks associated with the FIs' business operations;

iii. Ensure that all personnel and users are made aware of the applicable laws, regulations, policies, standards, guidelines, or procedures related to the usage and security of the FIs' IT systems and resources;

iv. Ensure that all personnel understand and are adequately trained to carry out their assigned information security-related duties and responsibilities. They should have at least adequate knowledge of the various management, operational and technical controls required and available to protect their IT resources for which they are responsible; and

v. Ensure that all personnel are kept up to date with the latest technology risks and cyber threats.

4. IT SYSTEM AND PROJECT

While keeping up with the latest technology development, the FIs might discover new technology that can further improve their business operation and process, and service delivery to the consumers. The FIs may want to implement the technology, in line with their IT strategy. However, the FIs should also be mindful that some technology, instead of becoming enablers which ease operations and functions, can turn into cause of concern for the FIs.

Planning is key for the success of the acquisition and development of applications. Ineffective technology implementation can lead to system ridden with errors or delays that may cause disruption to operations, so it is important to see major technology adoption or system acquisition and development as a project. Therefore, FIs should establish a project management framework to effectively manage IT projects in the FIs.

4.1 Identification of Critical System

4.1.1 FIs should put in place a framework and process in identifying their critical systems. A list of critical systems should be approved by the Senior Management and communicated to the Board.

4.1.2 The FIs should consider the need for diversity in technology and enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.

4.1.3 FIs should ensure their critical systems achieve high availability. Important factors associated with maintaining high system availability are ensuring adequate capacity, reliable performance, fast response time, scalability and swift recovery capability.

4.1.4 As technology and business operation evolve, criticality of system should be reviewed from time to time.

4.2 Project Management

4.2.1 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.

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

4.2.3 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.

4.2.4 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 IT and business unit.

4.2.5 FIs should incorporate risk management process to identify, assess, address and monitor risks that can adversely impact the IT project delivery timeline, budget and deliverables.

4.2.6 A project steering committee or equivalent should also be created that will manage the project according to the project scope, implementation plan and budget. The project steering committee should regularly update the ITSC on the status of the project. The project steering committee roles and responsibilities should be clearly defined.

4.2.7 A formal change management procedure should be devised by the project steering committee to identify and approve scope changes. The proposed changes should be properly documented, reviewed and approved by the project sponsor before it is implemented. Justifications on these changes should be made based on the relevancy to the project's core objectives, the risk factor of the proposed changes as well as evaluating the project's potential benefits against its potential costs.

4.2.8 Quality assurance should be performed by function or personnel of the FIs independent from the project management team to ensure project activities and deliverables comply with the policies, procedures and standards, and achieve the project objectives.

4.3 System Acquisition

4.3.1 FIs should understand the system that they wish to procure or develop, and prioritise their needs based on their business strategies and goals. Sufficient research and analysis as well as a financial evaluation to identify costs and benefits should be done to make sure that the application is really needed by the FIs and provides measurable benefits to them. The application should improve or enhance one of the following:

i. FIs' business operations;

ii. Quality of service to FIs' customers; or

iii. Internal decision-making.

4.3.2 FIs should have a framework for system or application acquisition and development that consider the following:

i. An effective and transparent procurement process;

ii. System Development Life Cycle model used by the FIs or vendors, which will include breakdown of all processes and tools required for each phase of the system acquisition and development.

iii. Align system acquisition and development project based on the FI's Project Management Framework to cover the allocation of responsibilities, activity breakdown, budgeting of time and resources, milestones, checkpoints, key dependencies, quality assurance, risk assessment, training and approvals amongst others; and

iv. Compliance with business and regulatory requirements.

4.3.3 FIs should have a systematic approach when procuring an application that involves the following:

i. Proper planning for the application needed by the FIs;

ii. Defining the requirements clearly in the Request for Proposal/Invitation for Tender;

iii. Appropriate tender selection and an effective evaluation procedure. The level of assessment and due diligence performed should be commensurate with the criticality of the project deliverables to the FIs; and

iv. Drafting a solid agreement that covers all the specified requirements with the successful tender.

4.3.4 Depending on the type of system acquisition, the FIs should also observe Paragraph 4.4, 4.5, 4.6 and 4.7 of this Guidelines, where applicable.

4.4 Off-the-Shelf Solution

4.4.1 If the FIs is planning to use an off-the-shelf solution, the FIs should ensure that the software version and license are for enterprise, commercial or business use.

4.4.2 The FIs should ensure the off-the-shelf solution does not reach or is almost reaching end of life or end of support. The latest stable version of the software is recommended.

4.4.3 Where possible, the off-the-shelf solution should be customised to tailor the FIs' requirements. This customisation should be implemented by the vendor during the acquisition and all changes should be recorded.

4.4.4 If the off-the-shelf solution does not meet the FIs' requirements, the FIs should assess the risks and ensure adequate mitigating controls are implemented to address the risks before the solution is deployed.

4.5 Open Source Software

4.5.1 If the system will be using open source software, the FIs should ensure that the software is developed by a reputable developer or online software community.

4.5.2 The open source software should be continuously maintained by the developer and/or online software community, especially bug fixes and security patches.

4.5.3 The open source software should be supported and/or well-funded by a trusted organisation or software community to ensure sustainability.

4.5.4 Where possible, the open source software solution should be customised to the FIs' requirements. This customisation should be implemented in-house or by software vendor during the acquisition and all changes should be recorded. A copy of the customised source code should be handed over to the FIs to be held securely from unauthorised access.

4.5.5 If the open source software solution does not meet the FIs' requirements, the FIs should assess the risks and ensure adequate mitigating controls are implemented to address the risks before the solution is deployed. If the risk gap can pose security risks or outweigh the benefits, FIs should consider another alternative solution.

4.6 System Development (Outsourced)

4.6.1 For system acquisition that require major IT application development, the FIs should ensure the application 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.

4.6.2 The FIs should ensure the application vendor has established a software development methodology such as SDLC or DevOps. The methodology should define the processes, procedures and controls at each phase of the project (e.g. initiation/planning, requirements analysis, design, implementation, testing and acceptance, etc.)

4.6.3 The FIs should adopt security-by-design or DevSecOps approach, which requires design and implementation of security in every phase of the software development project 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 project phases.

4.6.4 The FIs should identify, define and document the functional requirements for the system in the early phase of software development. In addition to functional requirements, key requirements such as system performance, resiliency and security requirements, should also be established and documented.

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

4.6.6 As part of the design phase, the FIs 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.

4.6.7 The FIs should 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.

4.6.8 Relevant functions and stakeholders should be engaged to participate in the design review. For example, the security design and architecture of the system should be reviewed by the FI's IT security function or a qualified security consultant.

4.6.9 The FIs should ensure a source code review on the application has been performed by an independent party, which can be either appointed by the FIs or the application vendor before the application is handed over to the FIs. The objective of this is to identify security vulnerabilities and deficiencies, and mistakes in system design, including defects due to coding errors, poor coding practices, malicious attempts, or unverified Programming Libraries.

4.6.10 A source code escrow agreement should be in place, based on the criticality of the acquired software to the FIs' business, so that the FIs can have access to the source code in the event that the vendor is unable to support the FIs.

4.7 System Development (In-house)

4.7.1 For FIs that develop major IT application in-house, the FIs should establish a software development methodology such as SDLC and DevOps. The methodology should define the processes, procedures and controls in each phase of the project.

4.7.2 The FIs should establish standards on secure coding, source code review and application security testing, and ensure the standards are applied throughout each phase, such as by integrating security-by-design or DevSecOps approach to the development methodology.

4.7.3 The secure coding and source code review standards should cover areas that include but are not limited to the use of secure programming functions and libraries, input validation, output encoding, access control, authentication, cryptographic practices, and error and exception handling.

4.7.4 The FIs is recommended to have full-time software developers that are trained to apply the standards when developing software. This is to ensure continuous maintenance and support of the software.

4.7.5 Relevant functions and stakeholders should be engaged to participate in the design review. For example, the security design and architecture of the system should be reviewed by the FI's IT security function or a qualified security consultant.

4.7.6 The FIs 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.

4.8 System Integration

4.8.1 System integration allows FIs to extend functionality of their system without having to acquire or develop another standalone system. When integrating a system with another system or component, the FIs should consider managing the integration project similar to system acquisition and development.

4.8.2 The FIs should ensure that the owners of both system including their vendors and relevant stakeholders are consulted for the integration. The owners of both systems should clarify the needs for the integration and ensure the understanding of both parties are aligned.

4.8.3 Both parties should define the requirements of the integration, assess the risks relating to the integration for both sides of the systems and plan strategies to address the risks.

4.8.4 FIs should study and carefully select suitable integration method and strategy for the system integration that commensurate with the risk and complexity of the systems and components (e.g. using middleware application, Application Programming Interface or API).

4.8.5 FIs should also plan how to address compatibility and interoperability issues prior to the integration and ensure data and controls in the system are streamlined. This includes but is not limited to the following:

i. Assess data structure and capacity of both systems;

ii. Assess potential changes to metadata where applicable;

iii. Optimise and test communication between the two systems or components;

iv. Ensure both systems are updated and security patches are installed;

v. Review user access matrix for the new components and data;

vi. Review security configuration of the new components;

vii. Prepare a testing plan that covers both systems, the components, and the integration tool; and

viii. Prepare a maintenance plan that covers the integrated system or components as a whole system.

4.8.6 For system integration to a third-party system, FIs should assess the third-party and carry out due diligence to ensure the third-party system is reliable and able to provide assurance that their system is well maintained and secure.

4.8.7 There should be Service Level Agreement (SLA) with the third-party to ensure the uptime, connectivity and security of the integrated third-party system are maintained.

4.8.8 The integrated third-party system should not be able to access or extract data directly from the FIs' main system, unless restricted on request and minimal basis.

4.8.9 The FIs should be mindful of the allowed financial services and activities within their license type and its relevant legislation. The system integration does not constitute handover of digital financial services.

4.9 System Testing and Acceptance

4.9.1 Testing is an important phase of application acquisition and development. Testing will help the FIs to look for errors and inconsistencies against the FIs' business practices with the application design. Users should be involved from the start of the project in order to gather their input and review on the user interfaces and help improve the application design.

4.9.2 A methodology for rigorous testing should be established which should cover functional testing, system testing, integration testing, security testing and acceptance testing.

4.9.3 A test plan should be established and approved before testing. The FIs should trace the requirements during the testing phase, and ensure each requirement is covered by an appropriate test case in the relevant test plan.

4.9.4 As user acceptance testing is critical, the FIs should prepare a testing strategy to cover almost real scenarios such as through black box testing and beta testing.

4.9.5 The concerned application can only go live once all the user acceptance testing is completed, and the project team is satisfied that it fulfils all of the requirements and is stable for daily use.

4.9.6 FIs should also perform stress-testing for their IT systems to ensure the specifications for the IT systems are sufficient to cater the demands and needs of the users and/or customers, especially in real live scenarios. This will help in identifying performance and quality issues that might arise when the system goes live.

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

4.9.8 The FIs 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.

4.9.9 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 FIs' operations or delivery of service to customers should be reported to the project steering committee and addressed prior to deployment to the production environment.

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

4.10 Bug Testing

4.10.1 FIs should have a process to continue test their system for bugs, even when the system has gone live. This will allow the FIs to proactively address functional and performance bugs or issues that could not be detect through scenarios of system acceptance testing.

4.10.2 FIs should analyse and resolve identified bugs by implementing software fix or patch on their system subject to their change management and patch management process.

4.10.3 FIs should provide a platform for customers to report application issues as customer complaints would be a useful channel to collect information about bugs. The reported issues should be analysed according to the criticality and reoccurrence.

4.11 Development Environment

4.11.1 FIs should set up development and/or testing environment for their IT system, IT infrastructure (i.e. server, virtual server, database) and IT assets (i.e. workstation specifically used for system access) for the purpose of development, modification and testing of FIs' IT systems.

4.11.2 Development and/or testing environments should be segregated from production environment so that any changes in development should not affect production environment. This can be done by deploying separate physical or virtual machine and applying network segregation.

4.11.3 User access control should still be applied on the development and/or testing environments. Software vendors' and developers' access should be recorded and reviewed.

4.11.4 Patch management should also apply to the development and/or testing environment. Any patching on the production environment should be applied on development and/or testing environment, unless required to test the application or to simulate specific system state.

4.11.5 As configuration management should also be applied to the development and/or testing environment, FIs should establish configuration baseline specific for development and/or testing environment, which may slightly differ from the production environment.

4.11.6 FIs should restrict the development and/or testing environment from directly accessing or operating any production environment.

4.11.7 Data in production environment should not be used in the development and/or testing environment. It is recommended to use dummy or simulated data; test data package or near-real data obtained via pilot or supervised testing.

4.11.8 If data from production environment is necessary in order to effectively test an application, the FIs is recommended to use the data temporarily for the testing purpose only and replicate the data on separate development and/or testing database. FIs should also ensure same level of security is applied on the development and/or testing environment as the production environments.

4.12 Web Browser

4.12.1 Depending on the type of the system, the FIs may use a web browser to access web applications and cloud applications. The FIs should specify a list of supported web browsers and its supported version, and ensure only fully supported web browsers are allowed.

4.12.2 FIs should also monitor and assess both the web application and web browser to ensure adequate performance and security, while maintaining compatibility.

4.12.3 The FIs should uninstall or disable any unnecessary and/or unauthorised browser extensions, plug-ins or add-ons.

4.12.4 The FIs should disable or block the following on the web browser, unless required by the web application:

i. third-party cookies;
ii. automatic storage of user credentials or password;
iii. website tracking;
iv. pop-ups; and
v. automatic download.

4.12.5 Features such as location services, camera and microphone should be made to should always require users' permission before use

4.12.6 The FIs should ensure that all system user accounts are logged out after every session or when not in use.

4.13 Artificial Intelligence

4.13.1 FIs that wish to implement artificial intelligence (AI) system for their business operation or service delivery should be mindful of other notices or guidelines issued by BDCB that are applicable to the activities involved in the AI system. The FIs should be able to demonstrate that the AI system will be able to maintain compliance to the notices and guidelines.

4.13.2 The FIs should ensure the AI system or application coding follows ethical standards and suitable best practices for software programming including ensuring the security-by-design approach is taken at every phase of the project.

4.13.3 The AI source code, feature engine and process flow should be made available for review and audit when required. The scope of this audit should include assessing fairness, privacy, security and transparency.

4.13.4 During the design phase, the FIs should plan a suitable and understandable analysis method that will be used by the AI. This should be supported with sufficient and relevant industry benchmarking, statistical or common trend analysis, and/or modelling in order to create suitable baseline for the AI system.

4.13.5 The AI system should be provided with sufficient near-real historical data to improve reliability of the analysis for the design and development.

4.13.6 The FIs should ensure any actions from the AI system are justified with response codes that describe the data and parameters used to come up with the concluded actions. The FIs should also ensure the actions are recorded and auditable.

4.13.7 The FIs should ensure there are means or methods for the FIs to make human intervention to the AI system when required. FIs should also be capable to roll back erroneous AI actions such as retract false approval and correcting falsely analysed data.

4.13.8 The AI system should be adequately tested on the development and test environment first and then against normal business process.

4.13.9 The adoption level of an AI system can be presented into the following:

i. Level 1: Reference
- Analysis of information based on pre-defined rules and set of answers
- Only provide information to support work only

ii. Level 2: Recommendation
- Processing information based on pre-defined rules and open answers
- Recommend actions for the human to consider

iii. Level 3: Prioritisation
- Automated rule-based processing
- Mainly to provide alerts and prioritisation but may run actions that do not involve major decision making

iv. Level 4: Scoring
- Analysis based on response and behaviour
- Use scoring before automatically applying rules and actions
- Able to predict data and forecast for human

v. Level 5: Adaptive
- Full-auto processing
- Able to learn behaviour, define patterns and adaptive

4.13.10 AI application on critical system should start at Level 1, Level 2 or Level 3 first, subject to the FIs' risk assessment.

4.13.11 Activity logs of all processes should be regularly reviewed to assess the accuracy and to correct error if any, until the error rate is 5% or below for at least 3 consecutive months before moving to Level 4 respectively.

4.13.12 AI system at Level 4 should be closely monitored for potential false positive. Transparency and user's consent are important as the AI system collect behaviour information of the users.

4.13.13 Before moving to Level 5, FIs should ensure the error rate of the AI system is no more than 1% over a period of 12 consecutive months while in Level 4.

4.13.14 FIs should ensure sufficient test results that meets the criteria above prior to implementing or moving to any level of the AI system.

4.13.15 When testing the AI system, reliable near-real data should be used to simulate real environment and the intended audience, which can minimise bias in the AI system. These data may be obtained from live test data in a controlled environment such as focus group or beta testing, or suitable data sets provided by reliable organisation.

4.13.16 As AI system are exposed to more data and use, the AI system may behave unpredictably over time from the new data patterns. Therefore, FIs should also periodically monitor the output of their AI system throughout the use of the AI system.

4.13.17 The FIs should also provide means for the users to provide feedbacks on the AI system including to report error, bias and suggest improvement to criteria used for data input.

4.14 Audit Trail

4.14.1 Establishing a proper trail process can greatly help in detecting security violations, performance problems and flaws in FIs' systems. This can be beneficial to FIs as it can help in achieving individual accountability, reconstruction of events, intrusion detection and problem analysis.

4.14.2 An audit trail should include sufficient information (e.g. logs) to establish what events occurred and who or what caused them.

4.14.3 FIs should consider in their system design plan and implementation measures that capture and maintain forensic evidence in a manner that maintains control over the evidence, and prevents tampering and the collection of false evidence.

4.14.4 In instances where systems and related audit trails are the responsibility of a third-party service provider or vendor, FIs should ensure the following:

i. FIs has independent or direct access to relevant audit trails; and
ii. The audit trails meet FIs' standards.

4.14.5 FIs should determine how long audit trail data will be maintained in accordance to the criticality of the systems, either on the system itself or in archive files.

4.14.6 Access to these audit logs should be strictly controlled and limited to the authorised personnel only.

4.14.7 FIs should implement measures that ensure the confidentiality as well as integrity of audit trail data, such as the use of encryption, digital signatures and strong access controls.

5. IT INFRASTRUCTURE AND OPERATIONS

The Senior Management should ensure the CIO is responsible for the oversight of the IT operations and is responsible to ensure that they have sufficient and reliable IT infrastructure, and an efficient and secure IT operations process. The CIO should also ensure information is stored in a timely, reliable, secure, and resilient manner. Daily operations are primarily the responsibility of the IT operations management team and they should ensure that the FIs has sufficient existing and planned infrastructure and adequate resources to accomplish their business objectives and IT goals.

Where some the IT infrastructure or IT operations are outsourced to a third party including as cloud services, the FIs should expect the outsourced party or cloud service provider to have similar or better level of resiliency and security as they would expect on their IT infrastructure and IT operation. The FIs should also observe the Guidelines on IT Third Party Risk Management (TRS/G-3/2022/2).

5.1 Data Centre Management

5.1.1 Critical systems that contain sensitive information and data should be located in a data centre. FIs should ensure that the data centre is resilient and the level of security and protection is sufficient against any threats, internally and externally.

5.1.2 Data centre should be located in a safe environment preferably in a less disaster-prone area. The FIs should ensure the surrounding of data centre is:

i. Above ground floor to avoid damage from flood;
ii. Away from water leak;
iii. Unaffected by building floor shock or vibration; and
iv. Away from electrical noise and heat pollution.

5.1.3 FIs should install sufficient physical facilities on the data centre to protect the servers and other equipment from environmental damage, including but not limited to:

i. Air-conditioning;
ii. Ventilation or filtering system;
iii. Humidity control;
iv. Raised floor;
v. Cable management; and
vi. Sufficient space between racks.

5.1.4 FIs should control and regulate the environment within the data centre by monitoring environmental conditions, such as temperature and humidity, within the data centre, promptly escalate any abnormalities to management, and resolve it in a timely manner.

5.1.5 FIs should implement appropriate fire prevention, protection and suppression measures in the data centre to control a full-scale fire if it occurs. For example, the FIs may consider the following, commensurate to the FIs' risk assessment and strategy:

i. install FM200 fire suppression system;

ii. install smoke detectors in the data centre;

iii. implement passive fire protection elements, such as fire- resistant materials around the data centre to restrict spread of a fire to a portion of the facility;

iv. provide handheld fire extinguishers for data centre personnel; and/or

v. provide fire marshal training for data centre personnel to ensure that they are trained to control a fire incident if it occurs.

5.1.6 In achieving data centre resiliency, FIs should assess, and where appropriate, install secondary power supply and data communications, and fault tolerance such as air conditioning, filtration systems, and fire suppression. This is to ensure that if one system fails, there is a backup to ensure there is minimal service disruption due to outage or damaged equipment.

5.1.7 FIs should ensure that there is sufficient backup power consisting of uninterruptible power supplies (UPS), battery arrays, and/or generator sets (GenSet) to ensure that critical systems continue to operate in case of an area-wide power outage.

5.1.8 FIs should ensure that the UPS has acceptable efficiency rate to regulate power in the servers and other vital equipment immediately during outage. The UPS should also have sufficient energy capacity to keep these servers and equipment running until GenSet is fully activated or failover to disaster recovery site.

5.1.9 FIs should ensure that these facilities and equipment are in good working condition by periodically performing testing and maintenance.

5.1.10 FIs should limit physical access to data centre to authorised personnel only. Access should be granted on a need-to-have basis. If physical access is no longer required, access to the data centre or server room should be immediately revoked.

5.1.11 FIs should have multiple security controls in place, where appropriate, to ensure authorised access to sensitive areas in their data centre, and for monitoring and recording activities that take place there. This should include but is not limited to having access controls, guards, surveillance tools, and intrusion detection systems to physically protect the sites at all times.

5.1.12 FIs should consider using appropriate authentication for access control to enter these sensitive areas. Identity checks should be in place to ensure the person who enters the facility has been authorised.

5.1.13 Appropriate security measures should be taken to ensure prohibited items are not brought into sensitive areas. Camera-embedded devices, removable media and USB drives should not be allowed to be brought inside the data centre to eliminate the ability for an attacker to introduce malware into servers.

5.1.14 For visitors such as vendors, engineers or personnel who do not have access to the data centre, but require temporary access in order to perform maintenance or repair work should formally submit access request to the FIs. FIs should ensure there is proper notification of and approval for the personnel for such visits during the specified duration of the activity.

5.1.15 FIs should ensure personnel and visitors do not bring in personal devices or equipment that can be connected to the servers, network or other equipment in the data centre unless declared as Bring-Your-Own-Devices (BYOD) under Paragraph 6.12.

5.1.16 FIs should ensure that visitors are accompanied at all times by an authorised employee while in the data centre. The FIs may provide a separate room near the data centre for development and deployment activities, and a working area for vendors or external parties to conduct troubleshooting or testing.

5.1.17 The FIs should ensure there are adequate physical security of the data centre to protect the FIs' servers and equipment from unauthorised access, including but not limited to:

i. Durable and lockable server rack;
ii. Access door with control access;
iii. Sufficient security cameras;
iv. 24 x 7 security personnel;
v. Viewing panel;
vi. Partition, enclosure and racks; and
vii. Thick wall or layered wall.

5.1.18 FIs are recommended to conduct a self-assessment or hire a third party to assess their data centre design and implementation based on any suitable standard or best practices, such as the Data Centre Resilience and Risk Assessment (DCRA), once every 3 years or a period according to the FIs' risk assessment including after major changes in the data centre

5.1.19 FIs should also develop IT asset and physical security review process on the data centre design. All components of the data centre design should be documented, safely stored and maintained.

5.2 Server Management

5.2.1 Servers are IT assets and should be managed according to Paragraph 6.2 on IT Asset Management.

5.2.2 The FIs should segregate Production server from Development and/or Testing server in accordance to Paragraph 4.11 on Development Environment.

5.2.3 Server operating system should be configured and hardened based on Paragraph 5.8 Configuration Management and Paragraph 7.11 on Anti-malware Solutions.

5.2.4 It is recommended for a server to be assigned with a single dedicated role (e.g. Web Server, Database Server) unless the additional role is required to be under same server (e.g. Domain Name Service and Dynamic Host Configuration Protocol).

5.3 Virtual Machine Management

5.3.1 Virtual server should be treated and configured similar as traditional server so Paragraph 5.2 on Server Management and Paragraph 5.8 on Configuration Management are applicable.

5.3.2 The FIs should define virtual machine (VM) templates that will be used to deploy new virtual servers or virtual appliance. The VM templates should be pre-configured and updated with latest security configuration.

5.3.3 As virtual server is stored as Virtual Machine (VM) Disk file, the VM Disk file should be uniquely named. The VM Disk file should be protected from unauthorised access and allocated in a secure drive and folder location.

5.3.4 Files, mounted ISO files or virtual drives that are not required should be removed from the VM datastore.

5.3.5 The operating system or firmware of the host virtual machine (VM) should be given additional attention. This includes but is not limited to implementing the following:

i. Limit accounts to manage host VM and the virtual servers;

ii. Limit network access on the host VM;

iii. Allow only authorised device to manage the host VM and virtual servers;

iv. Disable remote access to host VM or hypervisor; and

v. Patch the host VM regularly.

5.3.6 FIs should as much as possible ensure that compromise on one of the virtual servers should not have any effect on the host VM or other virtual servers, such as by limiting communication between the virtual servers and disabling file sharing.

5.4 Network Management

5.4.1 A holistic review of the FIs' network architectures at data centre, offices and other sites or branches should be performed to identify any potential single point of failure and weaknesses. FIs should implement appropriate measures to address and mitigate risk of disruption and compromise on their network.

5.4.2 To ensure network resiliency, the FIs may implement dual leased line or back up internet line (e.g. mobile broadband).

5.4.3 Communication between the FIs' branches and headquarters should be over a secured or dedicated line such as using leased line or Virtual Private Network (VPN).

5.4.4 The FIs should manage and control internet access based on their Acceptable Usage Policy. Network access on workstations used for critical systems should be restricted such as by implementing firewall, web filtering tools or web isolation.

5.4.5 The FIs should segregate the network to limit intrusion and manage access such as by implementing zero trust architecture, virtual local area network (VLAN), subnetting or guest network commensurate to the FIs' risks and complexity of their IT system and infrastructure.

5.4.6 FIs deploying Wireless Local Area Networks (WLAN) within the organisation should be aware of risks such eavesdropping and man-in-the-middle attack associated in the environment. Measures such as secure communication protocols for transmissions between access points and wireless clients should be implemented to secure the FIs' network from unauthorised access.

5.4.7 For data centres, the servers should be segregated based on their intended users. Demilitarised Zone (DMZ) should be set up for public-facing IT systems, while Production Zone should be set up for FIs' internal IT systems. The FIs can also create other network zones such as Testing and Development where necessary.

5.4.8 FIs should deploy network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical layers of infrastructure to protect the network perimeters.

5.4.9 For firewalls, FIs should create a firewall policy that specifies how firewalls should handle inbound and outbound network traffic. It is highly recommended that all inbound and outbound traffic not expressly permitted by the firewall policy to be blocked. Firewall policies should be monitored and reviewed periodically to ensure continued compliance with the FIs' relevant IT policies.

5.4.10 There should be a proper maintenance and review process for all network and security devices. Logs and alerts should be continuously monitored to identify threats. The software should be patched and updated regularly to address vulnerabilities.

5.5 Active Directory Management

5.5.1 FIs should manage the domain user accounts in the active directory based on Paragraph 7.1 on User Access Management including but not limited to segregating accounts into different account types and assigning based on least privilege administrative model.

5.5.2 FIs should not assign standard user accounts to the Domain Administrators group except default Domain Administrator account.

5.5.3 When an additional domain administrator account is required, an administrative level user account may be temporarily added into the Domain Administrators group for a certain period of time in order to perform the needed activity. This user account should be unique and an identifiable account.

5.5.4 The domain user accounts should be reviewed to ensure the right privilege is given at the specific period for a specific user account.

5.5.5 FIs should use a secure admin workstation or dedicated workstation to perform administrative tasks using domain administrator account.

5.5.6 Default or built in Domain Administrator account should be secured and the additional measures below should be applied, unless required by the FIs' system:

i. Enable the setting "Account is sensitive and cannot be delegated";
ii. Enable multifactor authentication to protect the account;
iii. Restrict network access on the active directory server;
iv. Disable log on as batch job;
v. Disable log on as a service; and
vi. Disable log on through Remote Desktop Protocol (RDP).

5.6 Database Management

5.6.1 FIs should use only authorised and supported Database Management System on a secure machine to manage the database.

5.6.2 All unnecessary services of features of the database should be removed or disabled.

5.6.3 Database Administrator should not be assigned with System Admin or SYSDBA role unless required to perform necessary system-level activities. All activities performed by the Database Administrator should be logged.

5.6.4 Database of each FIs application is owned by the respective System Owner. The System Owner must be kept informed of any changes performed to the database application.

5.6.5 Only authorised users are allowed to access or modify data depending on the business process of the System Owner's side. If Database Administrator requires privilege role that has access to view or modify data, authorisation from the System Owner should be obtained.

5.6.6 Default accounts (e.g. System Admin) must not be used for the production database management systems.

5.6.7 To further protect data at rest in the database, FIs may use encryption on database with critical and sensitive data.

5.6.8 Direct access to operating system level commands including stored procedures should be disabled or removed unless required.

5.6.9 The database production environment should be segregated from development or test environment so that developers for the system do not have access to live production environment. Test or development server and application should also not have access to production database.

5.7 Backup Management

5.7.1 FIs should develop an entity-wide data backup strategy for their critical system, which include storage and transportation of the backup data.

5.7.2 As part of the data backup and recovery strategy, FIs may implement specific data storage architectures such as backup tape, Network-Attached Storage (NAS) or Storage Area Network (SAN) sub-systems connected to production servers.

5.7.3 Depending on the risk, the FIs may implement more than one data storage media for backup. For example, a disk backup allows faster recovery than backup tape but may be exposed to similar threats as the server on-site. Moreover, some backup media may fail during restoration so an alternate backup will be useful.

5.7.4 FIs should carry out periodic testing and validation of the recovery capability of backup media and assess if the backup media is adequate and sufficiently effective to support the FIs' recovery process.

5.7.5 Backup tape should be stored off-site at a secure location based on the FIs' tape rotation procedure. The backup tape should be protected from unauthorised access, loss and physical damage.

5.7.6 The off-site location for backup tape should be located at least 5 km apart from the production data centre to reduce the exposure to similar geological threats.

5.7.7 FIs should encrypt backup media containing sensitive or confidential information before they are transported off-site for storage.

5.8 Configuration Management

5.8.1 FIs should determine configuration baselines for hardware and software used in the FIs. This is to ensure configurations are standardised and configuration loopholes are minimised. It is recommended to benchmark against industry best practices, security hardening guideline and this Guidelines.

5.8.2 FIs should also define configuration baselines to harden IT assets and IT infrastructure including server operating system, desktop operating system, databases, network devices, storage, enterprise mobile devices and BYOD within the IT environment.

5.8.3 Any unnecessary features or configuration options that are not required or used should be disabled such as unneeded programs and services in the server and unused physical ports on server or workstation.

5.8.4 As mentioned in this Guideline, FIs should have a proper inventory of their IT assets. This will be useful in determining the set of configuration items to be maintained.

5.8.5 FIs should have an on-going or continuous management and review procedure of the configurations. There should be regular configuration audits to ensure that secure configurations remain up to date and relevant, especially when there are change requests and upgrades to them. This ensures that the configuration baselines are applied uniformly and non-compliances are detected and raised for investigation.

5.8.6 Any deviation or exception to the configuration baseline should be assessed according to the risks and recorded in the IT assets register. Where possible, compensating controls should be apply to reduce the risks from the deviation or exception.

5.8.7 FIs should ensure that the frequency of configuration review and audits are commensurate with the risk level of systems.

5.9 Capacity and Performance Management

5.9.1 FIs should have a well-documented capacity management strategy that is regularly updated throughout the IT system lifecycle. FIs should plan for growth and change as well as taking into consideration the likelihood of an increase in their client-base or an expansion of their business operations.

5.9.2 FIs should have a platform that monitors the performance, capacity and utilisation of their IT resources and prepare strategy or plan to address performance issue or over utilisation of resources. This can reduce the risk of their systems reaching the performance, capacity and utilisation limit of their resources.

5.9.3 Predetermined thresholds should be established to ensure that the business units have sufficient time to plan and to procure additional resources to meet their operational and business requirements effectively. The performance monitoring platform should provide alerts or notifications once these resources reach the thresholds.

5.9.4 FIs should also monitor the availability of the server, network and services based on criticality of the system. The monitoring system should be able to detect when IT systems go offline. This provides the FIs with protection against hardware, software, and network failures while also being able to detect denial of service attacks. Availability monitoring could be implemented using network monitoring and network surveillance devices.

5.9.5 FIs should determine how systems should be monitored and what requirements to include when developing monitoring policies based on the criticality of the system. For example, critical systems with a high impact on the business operations of the FIs might need 24/7 real time monitoring.

5.10 Maintenance and Service

5.10.1 FIs should schedule, perform and document maintenance and repairs on IT asset in accordance with manufacturer or vendor specifications and the organisational requirements.

5.10.2 Maintenance contracts and warranty coverage and period should be included as part of the application acquisition and development. This will provide the FIs with prolonged support for any updates, coverage for any bug fixes and retraining if necessary.

5.10.3 FIs should control all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.

5.10.4 Maintenance should cover preventive maintenance and corrective maintenance, which should be performed by the vendors and/or IT personnel subject to the contracts.

5.10.5 Preventive maintenance should include but is not limited to the following:

i. Periodically inspecting, servicing, cleaning, or replacing physical components to prevent sudden failure;

ii. Monitoring of equipment to predict the limit of their serviceable life;

iii. Applying system upgrade, software updates and security patches subject to the FIs' patch management process; and

iv. Performing file housekeeping to support capacity and performance.

5.10.6 Corrective maintenance should be aligned with the FIs' IT incident process, which include but is not limited to the following:

i. Repair of equipment or replacement of components after a failure; and

ii. Repair of equipment or replacement of components to avoid reoccurrence.

5.10.7 The FIs should inventorise and plan replacement for devices or components that have become worn down due to wear and tear. The vendors should maintain a supply of expendable and critical components on-site so that these are readily available for corrective maintenance.

5.10.8 FIs should ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, FIs should clearly assign responsibilities to identified functions:

i. to continuously monitor and implement latest patch releases in a timely manner; and

ii. to identify critical technology systems that are approaching EOL for further action.

5.10.9 FIs should establish a patch and EOL management framework which addresses among others the following requirements:

i. identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems;

ii. conduct of compatibility testing for critical patches;

iii. specification of turnaround time for deploying patches according to the severity of the patches; and

iv. adherence to the workflow for end-to-end patch deployment processes including approval, monitoring and tracking of activities.

5.11 Log Management

5.11.1 FIs should identify logs that are important for security and troubleshooting of their system. These should include but is not limited to:

i. Any user access log;
ii. Operating System events logs;
iii. Network devices logs;
iv. Application and processing logs; and
v. Database query and job execution logs.

5.11.2 FIs should ensure the logs are enabled and relevant activities are recorded into the logs in the respective servers and devices. FIs should assess applicable legislation or regulation on log, record and/or data retention and to retain the logs for a period that is required by the applicable legislation or regulation.

5.11.3 As volume of logs can become large, the FIs should practise archiving the logs by using pre-built or third-party archive tools and to back up on another storage media.

5.11.4 FIs should ensure that the timestamp used for all logs are consistent, such as setting Network Time Protocol (NTP) with correct time zone.

5.11.5 Logs should be retrievable and readable, or at least certain part of the logs can be extracted into a readable format for common desktop application (e.g. PDF, Word, Excel, Text).

5.11.6 All logs should be protected from alteration or unauthorised removal. Access to the logs should be limited only to the designated administrator.

5.11.7 The logs should be reviewed periodically for monitoring and detecting suspicious activities such as cyber intrusion and fraud.

5.11.8 FIs should also generate periodic trends and statistic reports that should be used to review performance of the FIs' system and compliance to relevant IT policies and procedures. Logs are also an important source of information for incident handling and system enhancement planning.

5.11.9 Central log collection server is recommended to centralise common types of logs from different machines. The use of Security Information and Event Management (SIEM) or other similar tools can help the FIs to monitor and analysed logs more efficiently.

6. IT SERVICES AND END-USERS

IT is an essential part of daily business and operations for FIs. It has become a necessity as it increases productivity and eases business operations and processes. Role of IT to end-user is becoming important to support the success of the FIs business. Therefore, FIs should set up an IT service management framework for supporting their IT systems, services and operations.

6.1 IT Procurement

6.1.1 FIs should establish an IT procurement framework to manage purchase of software, hardware and services in the FIs. The framework can be aligned with the FIs' general procurement framework, project management framework and system acquisition process.

6.1.2 The procurement process should include due diligence, proposal evaluation and technical assessment. The process should also cover delivery of item, testing, deployment and verification, where applicable.

6.1.3 The FIs should determine vendors or suppliers that are authorised to provide hardware, software and IT consumables to the FI. This information should be included into the IT asset inventory list as stated in Paragraph 6.2 below and pursuant to the Guidelines on IT Third Party Risk Management (TRS/G-3/2022/2).

6.2 IT Asset Management

6.2.1 FIs should fully comprehend the whole nature of their IT operations and environment. An inventory list of their IT asset should be created to facilitate risk management procedures, control processes and maintenance of these resources. An inventory will be beneficial because:

i. It provides a record of valuable IT assets for tracking purposes;

ii. It helps to identify areas of potential risk;

iii. Support Business Continuity Management (BCM) planning; and

iv. It provides useful information during technical support or in the event of stolen equipment/theft.

6.2.2 The inventory list should include all computing and networking related resources owned, managed, or otherwise used by the FIs. This includes:

i. Software including product license/key;

ii. Hardware and appliances; and

iii. Warranty and other support contracts.

6.2.3 The inventory list should at a minimum consist of information that includes details of the IT assets such as asset tag, model and serial number, the location of these IT assets and the person who is responsible and held accountable for them.

6.2.4 The inventory list should cover IT assets at all FIs' offices, sites or branches in Brunei. The FIs should also account for information and associated assets stored in the cloud computing environment. This inventory list should be updated regularly and stored in a secure manner.

6.2.5 The FIs should identify which IT assets are critical based on the impact severity in the event these IT assets become inaccessible, loss, stolen or compromised.

6.2.6 The FIs should ensure all IT assets are subjected to regular firmware or operating system updates, bug fixes and security patches. The IT assets should also be maintained to keep the performance at satisfactory level.

6.2.7 For desktop and laptop, the FIs should install end-point protection such as anti-virus software to protect the desktop and laptop against malware. All software in the desktop and laptop including the end-point protection should be genuine and regularly updated.

6.2.8 All IT assets should be configured based on suitable configuration baseline as stated in Paragraph 5.8 on Configuration Management. Unused and unnecessary operating system features, protocol and ports should be disabled.

6.2.9 Considering the risks from the use of USB drives, the FIs are not recommended to allow USB drives on desktop or laptop that has access to FIs' critical system unless the USB drives are provided by the FIs or declared as BYOD.

6.2.10 All FIs' personnel should ensure IT assets are physically secured and to prevent unauthorised person from accessing or using these IT assets.

6.2.11 The FIs should establish procedures for its personnel to report damaged, lost or stolen IT assets to the IT team and police or other relevant authorities, where applicable.

6.2.12 The FIs should ensure there is a procedure in place to securely remove all information or data inside the IT assets before disposal or change of ownership.

6.3 Change Management

6.3.1 FIs should establish a change management process to ensure that changes to the production system are assessed, approved, implemented and reviewed in a controlled manner. An efficient and systematic change management process ensures that changes are made with minimum disruption to the IT services.

6.3.2 Due diligence should be performed before approving any changes to a system. Only authorised personnel are allowed to approve change requests.

6.3.3 Separation of physical or logical environments for systems development, testing, staging and production should be established.

6.3.4 Change management processes should apply to changes pertaining to the following items:

i. System and application upgrades, updates and patches;

ii. IT infrastructure designs and configurations;

iii. Hardware devices upgrades, updates and patches;

iv. Network controls and configurations;

v. Security controls and configurations;

vi. Changes to the surroundings (e.g. temperature, humidity, and airflow systems of the data centre); and

vii. Changes in technical documentation.

6.3.5 Upon receiving a change request, a risk assessment should be performed to determine whether the change is in the best interest of the FIs in relation to their current infrastructure, network and systems. FIs should ensure the changes would not cause major security and operational implications as well as address compatibility issues that might disrupt the existing production environment.

6.3.6 FIs should perform sufficient testing before implementing the changes to smoothen the change implementation on production environment. The FIs should verify with users of the system that there is no negative impact to their daily operation.

6.3.7 All changes implemented on the production environment should have detailed documentation that describes the change, the reasons for the change and how it is implemented. Test plans and test results with user sign-off should also be properly documented.

6.3.8 When implementing changes to a system, FIs should schedule it at a time when it has the minimal impact on their daily operation in relation to the usage of the affected systems.

6.3.9 Changes on the production environment should also be replicated and migrated to Disaster Recovery (DR) systems or applications for consistency.

6.3.10 Back-ups should be performed prior to any changes to a system. This allows FIs to have a rollback plan to revert to a previous functional version of the system if a problem arises during and after the deployment of the change. FIs should establish alternative recovery options to address situations where a change does not allow the systems to revert to a prior status.

6.3.11 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.

6.3.12 Urgent or emergency changes, that require the expedited implementation such as a high priority security patch for a system may not be able to follow the standard change management process. Therefore, FIs should prepare clear procedures for assessing, approving and implementing emergency changes, as well as designated the authorisers or approvers for the changes.

6.3.13 During urgent or emergency changes, the FIs should ensure all changes made can be tracked for documentation, which should be done after successful implementation of the urgent or emergency changes.

6.4 IT Helpdesk and Support

6.4.1 FIs should establish a focal contact point (i.e. IT Helpdesk or equivalent) for FIs personnel to make enquiry, request for technical assistance and report IT issue within the FIs.

6.4.2 The contact method and channel for the IT Helpdesk should be communicated to all personnel and should be accessible by all personnel at all offices, sites or branches of the FIs.

6.4.3 It is common for IT Helpdesk to be a first-level IT support in attending IT service request, providing technical assistance and resolving IT issues. The FIs should establish escalation procedure for the IT Helpdesk personnel to determine and inform the next level support or assistance.

6.4.4 These IT service request, technical assistance and IT issues should be recorded including the activities performed by the IT Helpdesk, escalations and actions taken.

6.5 Common Workstation

6.5.1 Some applications and peripherals are often shared for multiple users in the organisation on a common workstation within certain functions or within same workspace (sometimes referred to as terminal). The common workstation sometimes is used to segregate less restricted activities such as Internet or USB drive from other workstations. The FIs should ensure that this common workstation is protected from becoming an easy entry point for cyber-attack.

6.5.2 The FIs should protect the common workstation from unauthorised access such as by using login feature and to limit access only to relevant team. The use of the workstation should also be logged in case if a shared access is used, in order to identify users during a specific time.

6.5.3 There should also be additional security measures on the common workstation such as data housekeeping, operating system refresh or the use of sandbox session.

6.5.4 The common workstation should not be used for FIs system access and if possible, segregated from the same network zone.

6.6 Technology Refresh and Maintenance

6.6.1 FIs should prepare technology refresh and maintenance strategies that are driven by the business objectives and IT goals of a FIs. This normally includes maintaining security of IT systems and performance of IT assets so that they will continue to add value to FIs' operations.

6.6.2 The FIs should plan growth requirement and refresh schedule of their technology as their customer base increase and more new services provided by the FIs.

6.6.3 FIs should be proactive in managing IT resources and replace on a timely basis any outdated and unsupported systems, applications and software which significantly increase their exposure to security risks. FIs should pay close attention to the product's end-of-support (EOS) date as it is common for vendors to cease the provision of patches and fixes, including those relating to security vulnerabilities that are uncovered after the product's EOS date.

6.6.4 The FIs should conduct periodic analysis of IT resource historical performance including computing, network and storage utilisation trends.

6.6.5 Legacy systems or systems that are difficult to be replaced should be gradually replaced, subject to the risks posed by the legacy systems. Where legacy systems are still required to be accessed, it should have adequate compensating controls such as allowing access only within internal network and to implement stricter user account activity monitoring.

6.7 Online Web Services

6.7.1 The use of online web services is similar to using cloud services with Software-as-a-Service model (SaaS) since the system is hosted and managed by third party service provider. Online web services used for internal administrative and operational purpose should be declared to the FIs' IT team for assessment and authorisation.

6.7.2 Online web services that are authorised by the FIs should be recorded in the IT asset register similar to maintaining list of software.

6.7.3 The FIs should ensure that the online web services or SaaS is suitable for commercial used by subscribing with a commercial license instead of personal or consumer license where available.

6.7.4 The FIs should perform sufficient due diligence of the online web service provider including reviewing their privacy policy, user review and terms of use especially on their commitment to data security and privacy.

6.7.5 The FIs should be aware that not all security features on the online web services are enabled by default. FIs should explore and enable appropriate security features in the online web services (e.g. two-factor authentication, audit trail) as well as limit or disable unsafe features (e.g. limiting types of data collected for system enhancement).

6.7.6 If the FIs wish to use online web services or SaaS for critical business operation and in handling customer personal data, the FIs should refer to the Guidelines on IT Third Party Risk Management (TRS/G-3/2022/2) on Cloud Services.

6.8 Remote Access

6.8.1 Remote access allows users to connect to the FIs' internal network via an external network to access the FIs' data and systems, such as emails and business applications. Remote access should only be given to authorised personnel to perform activity that are approved by the IT team.

6.8.2 Remote access should be through encrypted connection (i.e. Virtual Private Network) to prevent data leakage through network sniffing and eavesdropping.

6.8.3 Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorised access.

6.8.4 The FIs should ensure remote access to the FIs' information assets is only allowed from devices that have been approved and hardened.

6.9 Virtual Meeting

6.9.1 FIs may use virtual meeting or tele-conferencing technology to communicate with other FIs personnel at different offices or branches, as well as external stakeholders at the comfort of each other's own premise. FIs should specify list of authorised application for the FIs employees to host virtual meeting.

6.9.2 Most virtual meeting application are offered as online web service or cloud application. FIs using these types of virtual meeting application should refer to Paragraph 6.7 on Online Web Services.

6.9.3 The FIs should prepare guidelines for its personnel on the etiquette and safe practices when hosting virtual meeting, especially to prevent unintended disclosure of information and data to unauthorised party during the virtual meeting.

6.9.4 The FIs should explore and recommend security features available on the virtual meeting application such as meeting PIN, multifactor user authentication and attendees' management dashboard.

6.9.5 The FIs may disable unnecessary features such as recording, gaining control over screen and file sharing unless required for certain type of meetings.

6.9.6 The FIs should ensure virtual meeting is only allowed from devices that have been pre-approved and secured.

6.10 Teleworking

6.10.1 There are times when the FIs require their personnel to be working remotely from home or other locations, such as when outstation and work travel. The personnel should be made aware that there are risks involved when teleworking and the personnel should adhere to any applicable policy or guidelines set by the FIs.

6.10.2 The FIs should provide guidelines for their personnel on how to secure their devices, network and environment when teleworking.

6.10.3 The FIs may also use secondary or alternate site for teleworking, or prepare list of authorised location for teleworking. Otherwise, the FIs may request the personnel to keep track of the locations where the personnel are working at.

6.11 Virtual Desktop

6.11.1 Virtual desktop allows personnel to access their computing resources on any laptop and desktop within the FIs with minimal hardware and software requirements through thin-client or zero-client technology. FIs should ensure decision to implement virtual desktop are support by justification including risk assessment and cost-benefit analysis.

6.11.2 As all computing resources are centralised, FIs should ensure there is an effective administration process for deployment of software, updates and configuration.

6.11.3 The virtual desktop should only be accessible on authorised IT assets within the FIs. Where required, access to critical or sensitive computing resources should be restricted to specific IT assets only.

6.11.4 As data are centralised on the virtual desktops' environment, there should be measures to ensure availability and recoverability of these data.

6.11.5 User access should be protected and where possible, to use multifactor authentication to strengthen the user access.

6.11.6 Access to virtual desktops should be through secure network link, preferably on a lease line within the FIs and through VPN. The network should also be stable and support load according to the number of full users.

6.11.7 FIs should on best effort ensure that any compromise on one of the virtual desktops will not cause adverse impact to other virtual desktops such as by disabling local hard drive, shared folder and USB drive.

6.12 Bring-Your-Own-Device

6.12.1 Depending on the FIs' risk appetite, some FIs may allow their personnel to use their personal devices for work. Such personal devices, especially if used for storing, processing and transmitting FIs data and connecting to FIs computing resources, should be declared as Bring-Your-Own-Device (BYOD) and recorded in BYOD inventory list.

6.12.2 The BYOD should be secured based on FIs' configuration baseline, patch management policy and anti-malware solutions, such as by ensuring the firmware and software are updated, anti-malware software is installed, and access require authentication.

6.12.3 The FIs should ensure the personnel will protect their BYOD from unauthorised access and to practice cyber hygiene for their BYOD.

6.12.4 FIs may use mobile device management system or other tools to help in tracking the BYOD, segregate personal data from FIs data and manage access or data in the BYOD.

6.12.5 The FIs personnel should inform loss, transfer of ownership and disposal of the BYOD to the IT team to ensure data is securely disposed and any link to FIs' systems are removed safely.

6.12.6 In the case of vendors or other external parties (e.g. auditors, visitors) bringing in personal devices to connect to the FIs IT computing resources, the vendors or other external parties should also declare their personal devices as BYOD unless a special arrangement is made to segregate the risks such as separate network for guest.

6.13 Internet-of-Things

6.13.1 FIs that uses smart equipment or appliances to store, process or transmit FIs data, or to connect to FIs' computing resources should be treated as an IT asset and recorded in the IT asset register.

6.13.2 Personal Internet-of-Things (IOT) devices should be regarded as BYOD if it is used to store, process or transmit data of the FIs and connect to the FIs computing resources.

6.13.3 The IOT devices should be from trusted manufacturer and the firmware are not hard coded so that firmware and software can still be updated.

6.13.4 The IOT devices should have security configuration menu that can be configured by the FIs such as in managing access control and network.

7. IT SECURITY

Information security is vital for all FIs as information or data is a key asset for all businesses. Protection of information or data is necessary to reduce the risk of losses from fraud, to ensure compliance with laws and regulations, to protect against any legal liability and to protect against any reputational risk that might have an impact on trust between the customers and the FIs. Security controls should be in place that prevent any data intrusion or unauthorized access and deliberate misuse or fraudulent changes. Effective security controls and measures are necessary to ensure the availability, reliability, recoverability and security of IT systems.

7.1 User Access Management

7.1.1 Access control limits the actions or operations that an authorised user of the FIs' IT system can perform. Users should only be doing specific tasks that they are assigned to, thus minimising the risk of a security breach. Three of the most common access control principles for protecting systems are:

i. Never Alone Principle: Certain functions in a system require more than one person at the same time, such as one person to perform action and another person to check. These functions may include system configuration change, password generation and access to administrative accounts;

ii. Segregation of Duties Principle: FIs should ensure that responsibilities and duties of personnel in the system are separated and performed according to their group role. The group should be able to perform all authorised functions, such as to enter, initiate, approve and execute transactions in a system. These functions include system changes on operating system, application coding, access control administration and backup data management; and

iii. Access Control Principle: FIs should only grant access rights and system privileges based on job responsibility and the necessity to have them fulfil a specific role. FIs should check that no person should have full rights to access any confidential data, applications, system resources or facilities in the FIs.

7.1.2 FIs should ensure that access to IT systems and IT assets are governed by a formally defined authorisation process covering the creation, modification, maintenance and deletion of accounts.

7.1.3 FIs should ensure that appropriate access rights or privileges of the assigned user are properly recorded and documented.

7.1.4 All users on IT systems and IT assets should be uniquely identifiable and their login activities should be recorded.

7.1.5 If access to the FIs' IT system is no longer needed, such as in the case of a user whose contract has been terminated, the account should be promptly revoked or suspended from the system. For FIs' personnel that are on an extended leave (e.g. maternity leave, study leave, etc.), their access to the IT systems should be temporary disabled until these personnel return to duty.

7.1.6 Users who are given access or privilege to FIs' IT systems and IT assets should be held responsible and accountable for their own account and to practice measures to protect their user accounts.

7.1.7 In assigning access, FIs should incorporate the principle of least privilege which grants the minimum level of access, rights, privileges and security permissions for the user to be able to perform their authorised tasks.

7.1.8 Access to privileged accounts should only be granted on a need-to-use basis and activities of these accounts should be logged and reviewed as part of the FIs' ongoing monitoring.

7.1.9 Non-employees should not be granted privileged account access unless written approval has been obtained from the FIs and they have signed a non-disclosure agreement. The request for access should justify the purpose of the request, the access level to be granted and the duration in which access is given to them.

7.1.10 FIs should enforce strong password controls over users' access to IT systems and IT assets. Password controls should include a change of default password upon first login, minimum password length and history, password complexity as well as maximum validity period.

7.1.11 To reduce risk of brute force attack on a user account, FIs may enforce periodic password change, unless multi-factor authentication is used to support the password.

7.1.12 FIs should perform regular reviews of user access privileges for their IT systems.

7.1.13 To maintain segregation of duties, the FIs should ensure the user role is independent and the permissions given for the role will not lead to conflict of interest such as between data entry and data verification role, or development and administration role in the IT system.

7.2 Data Asset Management

7.2.1 FIs should take a risk-based approach in managing their information and data, especially to ensure appropriate controls are in place for different types of data.

7.2.2 The FIs should establish data asset management framework that includes the following:

i. identification of information and data assets that support the FIs' business and delivery of financial services;

ii. classification of an information and data asset based on its risk, security classification and/or criticality;

iii. establishment of the ownership of information and data assets, and the roles and responsibilities of the personnel managing the information assets; and

iv. establishment of policies, standards and procedures to manage information and data assets according to their classification.

7.2.3 FIs' personnel should be aware of the information classification and to practise classification of their information. The FIs should also use security markings to let other personnel know the classification of the information and ensure the information will be handled properly by the personnel.

7.2.4 FIs should retain their data based on any applicable statutory or regulatory requirements for document retention, record keeping and information protection.

7.2.5 In the disposal of IT assets, FIs should ensure data are securely and permanently erased through various methods including data sanitisation, media degaussing and physical media destruction through incineration or pulverisation.

7.3 Data Security

7.3.1 FIs should develop a comprehensive data loss prevention strategy and adequate measures to address risks related to data breach, data theft and data leakage, taking into consideration the following:

i. Data at endpoint: Data that resides in laptops, desktops, portable storage devices and mobile devices. This should also include data residing on BYOD.

ii. Data in motion: Data that are transmitted over a network or transported between sites (e.g. back up tape);

iii. Internal data at rest: Data in storage devices that includes files stored on servers, databases, and backup media and storage platforms; and

iv. Cloud data: Externally stored data inside or outside the country.

7.3.2 Sensitive data residing on servers, database, endpoint devices and storage medias should be protected with strong encryption and access control.

7.3.3 Communications or transfer of sensitive information should only be conducted through encrypted channel or other secure means for information exchange as agreed with the sender/receiver. Alternatively, the FIs should encrypt the data before the transmission.

7.4 Cryptography

7.4.1 Cryptography is used as protocols for authentication, data encryption, digital signatures and in data integrity verification. When selecting encryption, FIs should adopt cryptographic algorithms endorsed and/or introduced by well-established international bodies such as Rivest-Shamir-Adleman (RSA) cryptosystem by RSA Data Security Inc. and Advanced-Encryption-Standard (AES) encryption supported by NIST.

7.4.2 The FIs should also define the appropriate encryption key length that meet its security objectives and requirements.

7.4.3 The FIs should ensure the selected cryptographic algorithms have been subject to rigorous testing or vetting to meet the identified security objectives and requirements.

7.4.4 The FIs should ensure encryption keys are securely generated and protected from unauthorised disclosure.

7.4.5 After a key is disseminated, the sender and receiver should destroy the media (e.g. envelope, e-mail) that are used to disseminate the keys.

7.4.6 Where encryption keys need to be transmitted, the encryption key of the data should be sent via a separate secure transmission channel to the intended recipients.

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

7.4.8 The FIs should remain up to date with any vulnerabilities relating to the encryption key and review the adequacy of the encryption key to ensure they remain resilient against evolving threats.

7.5 Security Monitoring

7.5.1 Continuous security monitoring is a vital aspect of technology risk management. FIs should establish appropriate security monitoring systems and processes that detect suspicious activities, sensitive data movement, threats and vulnerabilities on their information systems.

7.5.2 FIs should install security devices such as intrusion detection system and stateful inspection firewall, and security software tools such as file integrity checker and end-point protection manager to monitor security events in the system, network, application and end-point.

7.5.3 These security devices should have real-time monitoring as well as instantaneous alerts that are sent to the FIs' personnel if there are any suspicious activities or based on an appropriate threshold.

7.5.4 FIs should determine the monitoring requirements and analysis approach based on the complexity and criticality of the system, IT asset and data. For example, critical systems with a high impact on the business operations of the FIs might need 24/7 real time monitoring.

7.5.5 A process to collect, consolidate, process, review and correlate system logs should be established to facilitate FIs' security monitoring operations. FIs should regularly review security logs of systems, applications and network devices to detect any anomalies or suspicious activities.

7.5.6 The retention period of these logs should be considered based on any statutory requirements for document retention and protection. These logs should be retained and adequately protected to facilitate any future investigation.

7.5.7 To facilitate identification of anomalies, the FIs should establish a baseline profile of normal day activity. The profiles should be regularly reviewed and updated.

7.6 Threat Intelligence

7.6.1 FIs should subscribe to reputable threat intelligence services to identify emerging cyber threats, uncover new cyber-attack techniques and support the implementation of countermeasures.

7.6.2 FIs are also encouraged to collaborate and cooperate closely with relevant stakeholders and competent authorities in combating cyber threats and sharing of threat intelligence and mitigation measures.

7.6.3 FIs should also monitor threat intelligence from developer and manufacturer official support channel or community platform to keep abreast with vulnerabilities and patches specific to their system.

7.6.4 The FIs should establish a process to collect, process and analyse this cyber-related information for its relevance and potential impact to the FIs' business and IT environment.

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

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

7.6.7 The FIs should establish a process to detect and respond to misinformation related to the FIs that are circulated on the Internet and social media. These should be given attention as they may relate to an undiscovered or unreported issue in the FIs system.

7.7 Security Operations Centre (SOC)

7.7.1 FIs are recommended to set up a SOC to continuously perform the following functions on a 24 x 7 basis:

i. security logs and event management;
ii. incident coordination, analysis and response;
iii. vulnerability management;
iv. threat monitoring and intelligence management;
v. analysis of anomalies at endpoints and network layers; and
vi. perform other cybersecurity operations.

7.7.2 The SOC, whether managed in-house or outsourced to third party service providers, should have adequate capabilities and skilled resources to effectively perform the functions above.

7.7.3 The SOC should provide a regular report to the CISO, which include, at a minimum, the following:

i. trends and statistics of security events categorised by the type of attacks or potential attacks, target and source IP addresses, and criticality of system;
ii. information on emerging and potential threats to the FIs and recommendations to mitigate or prevent occurrence; and
iii. reviews of current cybersecurity posture of the FIs such as based on open vulnerabilities and unpatched system.

7.7.4 For in-house SOC, FIs should ensure the SOC is located in a physically secure environment with proper access controls. In most cases, SOC is usually within a restricted data centre area.

7.7.5 For a third-party SOC service, the FIs should ensure that the link between the FIs and the SOC are secured, preferably with a VPN tunnel.

7.7.6 A process should be established to ensure timely response, escalation and resolution of suspicious or anomalous system activities or user behaviour detected. The SOC should also have the capability to proactively block high risk activities and perform first-level incident response.

7.7.7 For FIs that cannot implement SOC, the FIs should ensure there are adequate real-time detection and analysis tools to be implemented with immediate alerts to the personnel on standby. Processes in handling such alerts should be in place to ensure appropriate response and actions are taken based on the severity.

7.8 Vulnerability Management

7.8.1 FIs should conduct vulnerability assessment (VA) on their IT assets including but not limited to their IT system, server, network and end-user computing to detect security vulnerabilities and weaknesses.

7.8.2 FIs should also carry out penetration testing (PenTest) on their system, server and network to conduct an in-depth evaluation of the security threats through simulations of actual attacks.

7.8.3 FIs should strategise the VA and/or PenTest based on the criticality and risks of each IT assets. For example, Internet-facing applications would pose the highest security risks from code injection, denial of service attacks and information leakage so both VA and PenTest would be applicable and should be more regular than other application.

7.8.4 The VA and PenTest can be done through the deployment of a combination of automated tools and manual techniques, or through a reliable security assessment service. Therefore, FIs should assess the tools and techniques that are best for their organisation and properly document them.

7.8.5 The scope of the VA and PenTest should be clearly defined and this should also include common and latest vulnerabilities relating to the IT assets. FIs should also refer to relevant standards or industry best practices such as OWASP and NIST SP 800-115.

7.8.6 The FIs should also assess and quantify the degree of risks for each vulnerability found from the VA and PenTest, and prepare timeline to address the risk based on the risk level of the vulnerabilities.

7.8.7 The FIs should implement an effective reporting and remediation process to fully comprehend the security threats, perform subsequent validation to ensure gaps are fully addressed and track unfixed issues, and determine accountability for all issues exposed by the VA and PenTest.

7.8.8 VA and PenTest should be conducted on a frequency commensurate to the FIs' risk and criticality of the system. However, VA and PenTest should be performed at least once before go-live and after any major change.

7.8.9 VA and PenTest should be done during a suitable time as not to disrupt normal business operation. Permissions from the Senior Management should be obtained before conducting VA and PenTest. Users and stakeholders of the concerned applications should also be informed before the testing is carried out.

7.8.10 If VA and PenTest are to be performed through security assessment service by a third party, the Guidelines on IT Third Party Risk Management (TRS/G-3/2022/2) would be applicable. Any information or data obtained during the testing will be treated as confidential so non-disclosure agreements should be signed between the FIs and the vendor.

7.9 Compromise Assessment

7.9.1 FIs with complex IT systems and infrastructure are recommended to perform a compromise assessment on their system, network and end-point at least once every two years. The purpose of this assessment is to detect previously undetected cyber intrusions or attacks in the system or infrastructure, such as Advanced Persistent Threat (APT) and surveillance program. The assessment will also help the FIs to determine any extent of damages from a successful cyber intrusion during the undetected period.

7.9.2 If there is evidence of cyber intrusion detected during the assessment, the FIs should immediately contain and eradicate the source of intrusion based on the FIs' cyber incident response process.

7.10 Patch Management

7.10.1 FIs should be aware of any updates and security patches available for hardware and software on their IT systems, IT infrastructure, IT assets and authorised BYOD.

7.10.2 All updates and security patches should be assessed and tested on development or testing environment prior to deploying them. This should also in accordance to the FIs change management process.

7.10.3 Security patches for vulnerabilities discovered from VA, PenTest, compromise assessment and cybersecurity incident may not be available immediately on the vendor, manufacturer and/or developer website. The FIs should report or submit support ticket on the vulnerability to the vendor, manufacturer and/or developer and to monitor new security patches released by them.

7.10.4 For authorised BYOD, the FIs should provide awareness on any new critical security patches to the employees and recommend them to apply the security patches as soon as possible.

7.11 Anti-Malware Solutions

7.11.1 Pursuant to the Notice on Early Detection of Cyber Intrusion and Incident Reporting (No. FTU/N-1/2017/1 and Notice No. TRS/N-1/2020/1), the FIs are required put in place early detection capabilities to detect cyber intrusion on their network, server and end-user computing. This should include detection of malware, so the FIs should install anti-malware solution on all servers and IT assets (i.e. end-user computing) used by the FIs.

7.11.2 The anti-malware solution should be configured to run active or on-access scanning on files download, removable storage, web page scanning and e-mail attachment.

7.11.3 The anti-malware database should be updated regularly, either automatically or subject to FIs' patch management process. As anti-malware solution may flag false-positive result and unintentionally block certain activities, the FIs should also establish process to review and manage false-positive result.

7.11.4 FIs should require their personnel to install anti-malware product on their authorised BYOD. If there is no anti-malware solution available for specific BYOD, the personnel should put in place other measures to secure their BYOD, which should subject to the FIs' IT team assessment.

7.11.5 Notwithstanding to the above, the FIs should also consider other anti-malware solutions to enhance detection capabilities and improve security of the FIs' IT system, IT infrastructure and IT assets subject to FIs' risks and complexity of the IT infrastructure. For example, end-point protection manager with agent, intelligent or behaviour-based security solution, ransomware protection and sandboxing.

8. IT INCIDENT

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. IT incidents can affect critical business operations including FIs' capability to deliver service to their customers and affect FIs' critical data. Therefore, it is important for FIs to establish an IT incident management framework to handle IT incidents, and to develop a business continuity plan to ensure the continuity of FIs' business operations and IT disaster recovery plan to ensure the recoverability of system and data.

8.1 IT Incident Management

8.1.1 FIs should establish a framework and process to manage IT incidents efficiently in order to minimise the impact from a prolonged disruption of IT service.

8.1.2 Roles and responsibilities of personnel involved in the incident management process should be clearly defined, and this should include recording, analysing, remediating, reporting and monitoring incidents. FIs should have an effective training plan for personnel that handles IT incidents.

8.1.3 The FIs should ensure their capability monitoring and security monitoring are effective so that early indicators can be detected and prompt measures can be taken to address the issues before they lead to an incident.

8.1.4 It is important that IT incidents are accorded with the appropriate severity level. As part of incident analysis, FIs may delegate the function of determining and assigning incident severity levels to a central IT helpdesk function. Criteria used for assessing severity levels of incidents should be established and documented.

8.1.5 FIs should establish corresponding escalation and resolution procedures where the resolution timeframe is commensurate with the severity level of the incident. The predetermined escalation and response plan for IT incidents should be tested on a regular basis.

8.1.6 The FIs should identify all stakeholders that may be involved in handling an IT incident including business units, vendors and Internet service provider.

8.1.7 FIs should ensure all IT incidents are recorded as IT incident report. The incident report should be assigned with reference number for easy and quick reference in case of similar incidents occur.

8.1.8 As incidents may stem from numerous factors, FIs should perform a root-cause and impact analysis for major incidents which result in severe disruption of IT services. FIs should include in its incident reports a summary of the incident, an analysis of root cause that triggered the event, its impact as well as measures taken to address the root cause and consequences of the event.

8.1.9 The root-cause and impact analysis report should cover but is not limited to the following areas:

i. Root Cause Analysis

a) Details of personnel who discovered and/or reported the incident;

b) Details on the nature of the incident;

c) Date and time when the incident happened;

d) Location of the incident including which system or IT assets are affected;

e) Details on why and how the incident happened; and

f) Brief details on similar incidents reported over the last 3 years.

ii. Impact Analysis

a) Extent, duration or scope of the incident including information on the systems, resources effectiveness and impact on customers;

b) Magnitude of the incident including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence; and

c) Breach of regulatory requirements and conditions as a result of the incident.

iii. Corrective and Preventive Measures

a) Immediate corrective action to be taken to address consequences of the incident. Priority should be placed on addressing customers' concerns and/or compensation;

b) Measures to address the root cause of the incident; and

c) Lesson learnt and measures to prevent similar or related incidents from occurring.

8.1.10 FIs should adequately address all incidents within corresponding resolution time frames and monitor all incidents to their resolution. The FIs should take remediation actions to prevent the recurrence of similar incidents.

8.1.11 The FIs 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.

8.1.12 The FIs should establish a communications plan that covers the process and procedures to inform its customers of downtime relating to the incident and resumption of the FIs' business operations.

8.2 Security Incident Management

8.2.1 In addition to IT incidents, FIs should establish comprehensive information security or cyber incident policies and procedures, or to incorporate cyber-attack scenarios into their IT incident management.

8.2.2 The policies and procedures should guide the FIs in taking appropriate responses during the cyber-attack scenarios including escalation processes and links to crisis response, business continuity and disaster recovery planning.

8.2.3 FIs should also prepare a clear communication plan for informing and engaging shareholders, regulatory authorities, customers and employees in the event of a cyber-incident. Where necessary, the FIs should promptly advise its customers on any actions that may be required on their part.

8.2.4 The cyber incident response policies and procedures should address the following:

i. Preparedness: Establish a clear governance process, reporting structure and roles and responsibilities of the cyber incident handling team as well as escalation procedures in the event of an incident;

ii. Detection and Analysis: Ensure effective and practical processes for identifying signs of compromise, assessing the severity of damage and root cause of compromise.

iii. Containment: Controlling the extent of damage and preserving sufficient evidence for forensics purposes;

iv. Eradication and Recovery: Identify and implement remedial actions to remove the known threats, recover the damages and resume business activities; and

v. Post-incident Activity: Conduct a post-incident review incorporating lessons learned and develop long-term risk mitigations.

8.2.5 All personnel involved in the cyber incident handling should be made aware of the incident response plan and handling procedures. The key contact person or an alternate person from the relevant functions should be contactable during an incident.

8.2.6 FIs should have an effective training plan for the IT and information security personnel that are involved in handling cybersecurity incident.

8.2.7 The FIs may identify and engage external assistance to support its resources to manage IT incidents. This is to ensure sufficient resources in term of facilities, expertise and tools are available to facilitate and support incident response and recovery. For example, the FIs can engage an incident response and security forensic company to support a cyber-attack investigation.

8.2.8 The FIs should ensure maintenance and protection of supporting evidence for the investigation of incidents, and for potential use for legal proceeding or criminal investigation.

8.3 Problem Management

8.3.1 FIs should maintain a record of past incidents which include lessons learned, to facilitate the diagnosis and resolution of future incidents with similar characteristics. A trend analysis of past incidents should be performed by the FIs to identify commonalities and patterns in the incidents.

8.3.2 Based on the trend analysis, the FIs should determine any recurring incidents and incidents with similar nature, in order to detect a common root cause or problem to these incidents.

8.3.3 The FIs should analyse the problem to determine the actual cause of the problem or gaps in the system, and determine further corrective or preventive measures, or workarounds.

8.3.4 The problem should also be rectified with vendors, suppliers, service providers, developers and/or manufacturers as the problem may be caused by unreported bugs, an undiscovered program flaw, weak vendor-recommended configurations and possible upgrades that were not informed to the FIs.

8.3.5 Problems that arise should be quantified based on their severity level. This allows FIs to effectively monitor and escalate the problems to the appropriate level, and establish an achievable target resolution time for each severity level.

8.3.6 Similar to incident management, problem management also requires FIs to keep record of logs that allows the FIs to look at the relationship between both incident and problem which is fundamental for the success of problem management.

8.4 Business Continuity Management (BCM)

8.4.1 FIs should have a comprehensive BCM program that includes a systematic process of resuming their critical operations and activities following a disaster or disruptive event such as downtime or cyber-attack, and an efficient process of restoring daily operations and activities after disaster recovery.

8.4.2 The Board are responsible for the approval and oversight of BCM program of the FIs. Senior Management should ensure the FIs establish and implement the BCM program.

8.4.3 The BCM program should include technologies and processes such as during failover process and back up restore process in the FIs that are necessary to maintain IT resiliency including ensuring availability, recoverability and reliability of IT systems, networks and infrastructure belonging to the FIs.

8.4.4 FIs should perform a business impact analysis to identify the different types of IT disruption or disaster that can affect the FIs, determine the impact to their business operations and the likelihood that the events might occur. This should include threat scenarios such as major system downtime, security incidents or disaster that prevent access to the FIs premise and its IT asset.

8.4.5 All systems, applications and services, including those provided by third-party service providers, should be identified and assessed. A risk assessment for each of the critical systems, applications and services should be conducted by the FIs to determine the possible implications to business disruption that may lead to other risk areas such as legal, operational and reputational risks.

8.4.6 A business continuity plan (BCP) should be established by the relevant business units that rely on IT systems, networks and computer resources. The BCP should be specific for each business unit and cover different processes in the business units. The business units should establish the minimal requirements and acceptable workaround to resume their critical processes.

8.4.7 The BCPs should be compiled by a BCM coordinator, who will oversee these BCPs and determine prioritisation based on the business impact analysis and risk assessments above. The BCM coordinator should understands BCM or be given relevant training where required.

8.4.8 Senior Management should periodically review the BCPs and the business units should update their respective BCP as and when there are changes to business operations, IT environment and threat landscape.

8.4.9 For FIs that have an alternate site or disaster recovery site for their BCP, the FIs should ensure the IT assets and infrastructure in the alternate site are well maintained and ready for use during disaster.

8.4.10 The BCP should be tested periodically in order to validate the effectiveness of the BCP and the ability of their personnel to execute the necessary procedures in the BCP. The testing should encompass different types of threat scenarios.

8.5 IT Disaster Recovery Plan

8.5.1 The FIs should perform a business impact analysis to determine its system recovery priorities in events where an IT incident leads to large scale service disruption. The FIs' systems' recovery time objectives (RTO) and recovery point objectives (RPO) should be defined according to its business needs.

8.5.2 The business impact analysis is vital in developing a disaster recovery plan. An effective disaster recovery plan allows the FIs to return to normal operations within a reasonable amount of time and minimise the amount of data loss for an IT system should a disaster or disruption occur.

8.5.3 The disaster recovery plan should cover strategies to recover IT systems in the event of a disruption or disaster and the restoration of the critical information systems that support FIs' business processes.

8.5.4 The disaster recovery plan should also cover post-disaster recovery activities, which includes returning back the IT systems and infrastructure to pre-disaster state (i.e. switch over back to production site).

8.5.5 The FIs' disaster recovery plan should include roles and responsibilities of relevant personnel and tools required during the recovery process.

8.5.6 In developing the disaster recovery plan, FIs should include the following measures:

i. The recovery of the data centre;

ii. The recovery of IT systems at the business location;

iii. The recovery of business operations and processes.

8.5.7 FIs should design an extensive plan for a rapid backup and recovery capabilities at each individual systems or applications. Some of the measures that FIs can implement to improve the recovery speed, the resiliency and robustness of their critical systems include:

i. Implementing alternative recovery strategies and technologies such as on-site redundancy and real-time data replication;

ii. Using service providers from different geological location for their backup strategies; and

iii. Using multiple network service providers and alternate network paths for network redundancy.

8.5.8 FIs should consider the inter-dependencies between critical systems when designing disaster recovery plan. This plan should also be formulated to address any reliance on third-party service providers or vendors and any other external dependencies required achieving recovery.

8.5.9 The alternate or disaster recovery site of data centre should be geographically separated at the minimum five kilometres apart from the main primary site. This should allow FIs to restore their critical systems and resume business operations on that site when the primary site goes offline due to a disruption or external event.

8.5.10 The disaster recovery plan should be periodically reviewed and updated when there are material changes to business operations and information assets.

8.5.11 During the recovery process, the FIs should only follow the established disaster recovery plan that has been tested by the FIs and approved by the Senior Management. FIs should avoid taking untested recovery measures which are likely to carry higher operational risks.

8.5.12 The FIs 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 ensure FIs system can perform as expected.

8.5.13 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.

8.5.14 The testing of disaster recovery plans may comprise:

i. various disruption scenarios, including full and partial shutdown of the primary site and major system;

ii. recovery dependencies between information assets, including those managed by third parties; and

iii. testing of its disaster recovery site based on normal business operation to gain the assurance that its disaster recovery site is able to support business needs.

8.5.15 Where IT assets used for disaster recovery (DR IT assets) are managed by service providers, the FIs should ensure the DR IT assets are also tested and verified to meet its business needs. The FIs should also participate in disaster recovery testing conducted by the service providers especially if bilateral or multilateral recovery testing efforts are required.

8.6 Crisis Management

8.6.1 In some situations, major incidents may further develop into a crisis. The Board and/or Senior Management should be kept apprised of the development of IT incidents so that the decision to activate crisis management can be made on a timely basis.

8.6.2 Crisis management aims to minimise impacts or damages from a major IT incident, as well as to facilitate and expedite incident handling process, business continuity plan and disaster recovery plan. The FIs should also engage further assistance from external subject matter experts to manage a crisis and resolve major IT incidents.

8.6.3 Being able to maintain customer confidence throughout a crisis or an emergency situation is important to the reputation and soundness of the FIs. FIs should include in their crisis management procedure a predetermined action plan to address public relations issues as well as to keep customers well-informed of the major incident.

8.6.4 The FIs should establish a communications plan that covers the process and procedures to handle any media or public queries relating to the IT incident. The FIs should identify the spokespersons and subject matter experts to address the media or public queries as well as the platforms to disseminate information.

8.7 Cyber Exercise

8.7.1 FIs 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 simulation, table-top exercise, or cyber drill.

8.7.2 The threat scenario should be designed based on real cyber incidents. As an alternative, the FIs could also design the exercise scenario by using threat intelligence that is relevant to their IT environment.

8.7.3 Depending on the exercise objectives, the FIs should involve relevant stakeholders, including senior management, business units, corporate communications, crisis management team, service providers, technical staff, head office and branches. This can be done all at one time or through a series of exercise sessions.

8.7.4 The test scenarios of the cyber exercise should be designed to test:

i. the effectiveness of escalation, communication and decision-making processes that correspond to different impact levels of a cyber-incident;

ii. the readiness and effectiveness of cybersecurity incident handling team and relevant service providers in supporting the recovery process; and

iii. the effectiveness of relevant standard operating procedures relating to the system including business continuity plan and IT disaster recovery plan.

8.7.5 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 of business units to ensure the activities do not disrupt the FIs' production systems.

8.7.6 At minimum, the cyber exercise can be conducted as a table-top exercise where all relevant stakeholders gather together to discuss the scenarios and go through their incident handling process. For more effective testing, the FIs should also consider walkthrough, simulation and red teaming exercise.

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

i. severity assessment and classification of an issue;
ii. timeframe to remediate issues of different severity; and
iii. risk assessment and mitigation strategies to manage deviations.

9. DIGITAL FINANCIAL SERVICES

Financial consumers are becoming more aware of technology and digital channels have become more preferred by consumers to access financial services. Considering the demand, more FIs have shifted to digital financial services. However, considering digital financial services are offered over digital or electronic channels, it is important for the FIs to ensure their IT system and services are secured from online criminals and operating and performing reliably.

9.1 Payment Cards

9.1.1 Risks associated with payment cards include lost card, card theft, counterfeit card, identity theft and payment fraud. FIs should implement sufficient security controls and measures to protect sensitive payment cards data. Data should be encrypted to ensure the security, confidentiality and integrity of payment cards data.

9.1.2 FIs should also have a secure payment cards system and networks to ensure these data will not be intercepted during the processing of sensitive and confidential information.

9.1.3 FIs should implement EMV standards on the payment cards and terminals they issue to ensure sensitive customer data is kept and transmitted securely.

9.1.4 FIs should have a secure card activation procedure once a payment card is distributed to the card holder. Such activation procedure can be conducted via FIs' mobile application or online services portal such as through in-app prompts or in-app live chat, In addition, the FIs may also provide multi-function machine or kiosk for card activation, or allowing customer to contact the FIs via official hotline or in person for the card activation.

9.1.5 It is highly recommended for FIs to implement a multi-factor authentication (e.g. online OTP or SMS OTP) for card-not-present transactions via internet to reduce fraud risk associated with such transactions.

9.1.6 FIs that provide payment card services should implement effective fraud detection and granular transaction monitoring systems. These should focus on pattern and behaviour modelling of transactions, and should be capable of detecting fraudulent use of a cardholder's account or payment cards.

9.1.7 FIs should follow up on any transactions made by their customers that exhibit behaviour that deviates significantly from a cardholder's usual card spending patterns. The cardholder should be contacted and FIs should confirm that they are genuinely making these transactions and then obtain their authorisation prior to completing the transaction.

9.1.8 FIs should ensure their system will promptly notify and alert a cardholder whenever a transaction is made with their payment card regardless for withdrawal, payment or deposit. This is to avoid disputes by customers especially when customers claim the payment is not conducted by the cardholder.

9.1.9 In the event it has been verified that a payment is not conducted by the cardholder, FIs should have a process in place to notify the customer to lodge report to the Royal Brunei Police Force and assist with the investigation where necessary.

9.2 Payment Terminal

9.2.1 FIs that procure payment terminals should ensure its terminal, application and processing system comply with the minimum requirement such as PCI-PED (if applicable), PA-DSS and PCI-DSS. It is expected for FIs to conduct a periodic review of all its terminals to remain in compliance as standards do change over time.

9.2.2 Prior to offering a payment terminal to any merchant, FIs should conduct proper due diligence on its merchant during on-boarding to prevent misuse and to protect the payment terminal.

9.2.3 It is also expected for FIs to maintain a list of all terminals used by their merchants including type of subscription, terminal deployed, when it was provided to the merchant and last date of inspection.

9.2.4 FIs should be able to monitor the condition and status of its terminals to ensure its terminals are not defected. The FIs should also regularly inspect the terminal used by any merchant to ensure it is not tampered or modified.

9.2.5 Payment terminal offered by FIs would usually depend on a stable network connection for a successful transaction. With this, the FIs should ensure their payment terminal network is secured and maintained. The FIs should also advise the same to its merchant in terms of maintaining their network.

9.3 Multi-Function Machine (MFM)

9.3.1 MFM includes Auto-Teller-Machine (ATM), Cash Deposit Machine (CDM), Cheque Deposit Machine (CQM) and Coin Deposit Machine (CoinDep). Although it provides customers to do banking transaction without human interaction, FIs should be concern of the technology risk associated with such initiative.

9.3.2 FIs should ensure its MFM remain compliant to PCI-DSS at a minimum, and should be upgraded on a timely basis to comply with the latest requirements. For FIs that offer CoinDep, compliant to PCI-DSS, it is recommended if the machine requires users to insert their debit/prepaid card.

9.3.3 FIs should install the latest security features on its machine such as anti-skimming devices, encrypted PIN Pad and hidden camera.

9.3.4 FIs should maintain a list of all its MFM whether on or off premise (i.e. branches, standalone MFM).

9.3.5 FIs should monitor the status of the MFM to detect downtime and performance issues. It is encouraged for FIs to conduct regular maintenance and testing especially on the performance of all its machine and update/patch whenever available.

9.3.6 In order for FIs to maintain cash at its ATM at all time, FIs should also monitor the cash level in its ATM and provide an alert to the FIs when the cash reaches a certain threshold.

9.3.7 For payment or transfer of funds via ATM/CDM, when customers input the receiver's account number, to prevent the wrong transfer of funds, the FIs may allow customers to view certain, but limited, details of the receiver such as the individual's first name or a part of the company name that will receive the fund.

9.4 Online Payment Gateway

9.4.1 FIs that offers Online Payment Gateway to its clients should conduct proper due diligence during the on-boarding process to prevent misuse and to ensure whether the customer is capable to use the service competently.

9.4.2 It is also expected for FIs to conduct a review on all of its clients that have opted for such service to confirm if the clients still require the service.

9.4.3 Prior to offering Online Payment Gateway, FIs should conduct its own risk assessment in terms of integrating into the FIs' IT system and the capability of the FIs to address any issues arising from such service.

9.4.4 Similar to other technology and innovation introduced by the FIs, it is expected for FIs to remain compliant to PCI-DSS requirement and to regularly review their service to ensure compliance to standards.

9.4.5 Performance and security of the Online Payment Gateway service is important to the client, so the FIs should ensure the system is maintained and secured, such as by applying regular updates and security patches.

9.4.6 FIs should maintain a log for any change or update on its Online Payment Gateway for the purpose of audit.

9.5 Online Financial Services

9.5.1 Online financial services refer to services offered by FIs on the Internet via web application or online portal. As such, FIs should implement security and control measures that are commensurate with the risk involved to ensure data confidentiality, integrity, availability and resilience of the online services.

9.5.2 In order to have a secure authentication system in place, FIs should consider the following measures:

i. Allow users to choose a longer login password (e.g. up to 12 characters) including alphabet, numerical and special character unless supported with two-factor authentication;

ii. Provide options to show users how long the password has been in use and to recommend a password update when it reaches a certain period;

iii. Allow a limited number of login attempts and if the user fails to enter the correct login details, the online account should be disabled for a certain period to prevent brute force dictionary attack;

iv. FIs should also have multi-factor authentication for logging into the online systems;

v. Double confirmation whenever a customer wants to authorise an online transaction (e.g. transferring money, bill payment and cash top up);

vi. Automatic logout after a period of inactivity or when web browser is closed; and

vii. Transmission of sensitive data on the internet should be done via secure and encrypted communications.

9.5.3 FIs should secure communication channels by using strong cryptographic controls to safeguard the confidentiality and integrity of confidential data during transmission such as using Secure Socket Layer (SSL) or Transport Layer Security (TLS) encryption.

9.5.4 FIs should take adequate measures to minimise exposure to its online financial services from any cyberattack such as code injection attack, distributed denial of service (DDoS) and spoofing attacks.

9.5.5 FIs should provide an option for customers to subscribe to transactions alert (SMS, email, mobile banking) for any account information changes or transactions conducted over the online financial service.

9.5.6 FIs should also perform regular and rigorous testing on the web application or online portal including end to end process and transactions. It is also expected for FIs to maintain a log for any change or update to system interface, process and security features of the web application or online portal for audit purposes.

9.6 Mobile Application

9.6.1 FIs that offer online financial services access via smartphones or tablet devices should be aware of the risks unique to mobile applications. As such, FIs should implement specific measures aimed at addressing risks of offering mobile applications.

9.6.2 FIs that offer mobile applications should consider additional measures to enhance security of the application, for example as follows:

i. Disable storing or caching data in the mobile application or to clear the data when session ended. If storing of data is necessary for the application, the data should be stored in the local storage of the device instead of sending over to the server, and to be protected using end-to-end encryption;

ii. Implement appropriate application integrity checks to verify the authenticity and integrity of the application;

iii. Implement a secure in-app keypad to mitigate against malware that captures keystroke; and

iv. Implement device binding to protect software token from being cloned.

9.6.3 FIs should continuously monitor the status of its applications, regularly conduct vulnerability scanning and penetration testing, and perform security update/patching when available.

9.6.4 When there is an update or new feature being introduced in the mobile application, FIs should perform focused testing as well as beta testing. The main objective of such testing is to ensure all issues are resolved prior to launching of the new feature or update rather than focusing on a scripted scenario.

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

9.7 E-Wallet

9.7.1 For FIs that are venturing into offering e-Wallet service, it is expected for the FIs to conduct its own risk analysis in terms of its IT system, infrastructure and the capability of the FIs to address issues arising from such service.

9.7.2 For FIs that are currently offering e-Wallet to the general public, FIs should assess and be mindful of the additional risks associated with it such as loss of money stored in the wallet, unauthorised transactions or unsuccessful transactions.

9.7.3 To address the abovementioned risks, FIs should ensure there are adequate controls in place on the e-Wallet interface at customer level and merchant level, which includes secure connection between e-Wallet and bank/card service provider, periodic review on the application and security testing.

9.7.4 FIs should provide an option for customer to receive notifications including but not limited to failed transaction, successful transaction, receiving funds or top ups, change in password or insufficient balance.

9.7.5 Access to e-Wallet and transaction confirmation should be protected with authentication such as PIN and device biometric.

9.7.6 Bank account and card information stored in the e-Wallet whether it is on the device or server should be encrypted. At the application user interface, the information should be partially masked.

9.7.7 Prior to offering e-Wallet payment services to any merchant, FIs should conduct proper due diligence on its merchant during on-boarding to prevent misuse.

9.7.8 Performance of the e-Wallet would usually depend on the device specification and a stable connection for a successful transaction. With this, the FIs should ensure their e-Wallet payment network is secured and maintained. The FIs should also advise its merchant in terms of maintaining their device and network.

9.7.9 FIs should maintain a list of all merchants using the e-Wallet services and to regularly monitor the usage to prevent tampering or modification on the e-Wallet application.

9.8 Open API

9.8.1 Considering API involves integration to a third-party system, FIs should consider Paragraph 4.8 on System Integration. FIs should evaluate if the API should be offered as Private API or Open API based on the risks of the integration. In the case of Open API, the API functions should be limited to public information access, read-only or one-way processing using response or status code.

9.8.2 When providing Open API to the public, the Open API should only be released on the FIs' official website and/or authorised third-party official website. The download page should be included with clear terms of use and sufficient documentation for the developer.

9.8.3 FIs that offer Open API whether it is available on the FIs' website and/or other third-party's official website, should take the following measures:

i. Ensure data for the API are separated from the main database;
ii. Where possible, to restrict response as codes or instructions only;
iii. Use session for each request in the API;
iv. Data given from the API should be stored temporarily on a need basis only; and
v. Data should be cleared when session is terminated or idle after a certain period of time.

9.8.4 FIs is responsible to inform their customer that the customer will be visiting a third-party API when transitioning into the Open API.

9.8.5 FIs should record who has downloaded and integrated the Open API into other system such as by requiring the third-party to provide registration details before downloading their Open API.

9.8.6 FIs should also keep track of what information is being shared to the third-party and perform a periodic review on the use of their Open API to ensure the usage is still applicable. Where possible, the FIs should be able to monitor and disable misuse of the Open API.

9.8.7 The Open API should be updated regularly to fix bugs and vulnerabilities. Any updates should be communicated to the third-party and on the download page. The FIs should also be able to disable obsolete version of the Open API.

9.9 Robo-Advisory

9.9.1 Prior to introducing Robo-Advisory to the public, FIs should conduct its own risk assessment in terms of IT system, infrastructure and the capability of the FIs to address any issues arising from such service.

9.9.2 Robo-advisory that provides service advisory supported by AI should be regarded as AI system. As such, the FIs should inform the customers that they are interacting with an AI and to remind them that the results provided should be use as guidance only. Customers should be advised to consider other factors before making decision or committing to products or services offered by the FIs. Please refer to Paragraph 4.13 on Artificial Intelligence for more information.

9.9.3 The Robo-Advisory should only provide guidance and reference for the customer to support decision making. It is not recommended for the Robo-Advisory to make decision or perform action on behalf of the customers without human intervention.

9.9.4 Any action or decision making following to advisory is considered as another type of process or operation taking place, such as on-boarding or payment. The FIs should refer to any applicable BDCB notices and guidelines relating to the process or operation, as well as to consider Paragraph 4.13 on Artificial Intelligence if the process is automated.

9.9.5 For FIs that venture into utilising Robo-Advisory for a limited purpose such as comparing insurance or takaful product, assessment of customer's risk profile and assessment of customer's credit application, the FIs should put in place measures to enhance security and protection of customer personal information, for example as follows:

i. Personal information or data should not be stored after the advisory session ends unless new process take over, which Paragraph 4.13 on Artificial Intelligence and Paragraph on 10.1 Consumer Personal Data Protection would be applicable.

ii. Clear information or data that has be cached after the session ends;

iii. There is human intervention when authentication and verification of its customer is necessary; and

iv. Assessment on customers remains the responsibility of the employees and subject to other applicable processes, which is beyond advisory.

9.9.6 The rules used for Robo-Advisory analysis and recommendation should be similar as to how FIs would normally conduct in-person. Where Machine Learning is used to provide advisory services based predictive machine learning algorithm, the FIs should ensure that they will be able to monitor the pattern and have manual intervention processes in place.

9.9.7 In ensuring the Robo-Advisory remains relevant and applicable, regular review and testing should be conducted. FIs should also be able to analyse the Robo-Advisory outcome that resulted in customer's dissatisfaction or being incorrectly advised for the FIs to better enhance such service.

9.10 Chatbot

9.10.1 Chatbot can be considered as an alternative form of general communication with the FIs and is useful during non-working hours or facilitate high volume of customers. FIs that introduce this type of communication may either embed it into its website, mobile application or Kiosk.

9.10.2 The chatbot should be used for providing information and support on certain feature such as how to request for refunds, conduct transaction, reviewing accounts and offer feedback. FIs should ensure the information that will be provided to its customer are correct, relevant and transparent to their request.

9.10.3 As such, FIs should regularly conduct a review and testing to ensure information or query requested by the customer is relevant and applicable.

9.10.4 For FIs that introduce a chatbot option, the following security measures should be considered:

i. No customer information or data is to be stored after session ends;
ii. Disable caching information or data; and
iii. FIs to maintain a record on the decision made by the customer.

9.10.5 FIs should be able to provide the option for Live Chat with an FIs representative or at least provide the FIs' official contact details for the customers to contact should the information or query does not meet the expectation of the customer.

9.11 Social Media

9.11.1 FIs often use social media to promote financial products or services, and to make latest announcements relating to their business. Considering social media is powered by a third party, FIs should evaluate the risk and determine which social media is suitable for the FIs.

9.11.2 Similar to FIs' official website, social media should only contain information that can be released to the public.

9.11.3 The social media account should be a business account and recommended to be verified if available on the chosen social media platform.

9.11.4 The content of the social media should only be managed by the content administrator. Access to the social media account should be limited to the content administrator.

9.11.5 The social media account should only be used for the business or corporate purposes. The account should not be used for personal purposes and linked to other unrelated services or websites.

9.11.6 Unnecessary features in the social media platform should be disabled, such as personalised advertisement and auto collection of diagnostic data, where the options are available.

9.11.7 The FIs should monitor and control the profiles followed, friends added, pages liked or groups joined. Where possible, the FIs should review their account's followers or friends, and remove or block fake followers or friends.

9.11.8 Comment features should be disabled unless administered by the content administrator. Comments that are potentially harmful or illegal should be removed.

9.11.9 The FIs should provide official contact details on the social media. If the FIs allows instant messaging (IM), direct messaging (DM) or other built-in messengers, the FIs should ensure there is dedicated personnel to answer the online queries. Where possible, the FIs should direct the public to the official contact channel for further information.

9.12 Kiosk

9.12.1 For FIs that are considering to offer Kiosk services, the FIs should consider the available technology in the market, human resource including expertise, network connectivity and FIs' strategic direction.

9.12.2 For FIs that currently offer Kiosk to the public, the FIs should conduct its own risk assessment in terms of IT system, infrastructure, resources and capability to support such initiative.

9.12.3 FIs should ensure there are sufficient security controls and measures in place such as but not limited to the following:

i. Closed-circuit television (CCTV) to be installed near the Kiosk;

ii. No customer information or data should be stored after each session ends;

iii. Disable physical access to the Kiosk's CPU or back-end hardware;

iv. Disable access to the operating system, firmware and other application in the Kiosk;

v. Provide alerts to customer in case of certain items (e.g. identity card, ATM card) are not removed properly; and

vi. FIs to maintain a record on the decision made by the customer for review purposes.

9.12.4 FIs should periodically update and upgrade its Kiosk to maintain good security and performance. FIs should also have an online monitoring mechanism that will be able to detect if a specific Kiosk is unresponsive due to hardware issues, damages or malfunctions.

9.13 Biometric

9.13.1 The use of Biometric for Digital Finance Services refers to an alternate method of identification and authentication to gain access to FIs' services such as mobile application and Kiosk; verifying transaction or confirming payment.

9.13.2 Biometric can be in a form of individual's face feature, iris, voice recognition or fingerprint. Whether this is captured by FIs' application or customer's device, FIs should address specific concerns and risks associated with the use of Biometric.

9.13.3 It is recommended for FIs to implement security controls and measures, for example as follows:

i. There is a consent made by the individual to use their Biometric for access, verification and confirmation;

ii. Allow users to choose a longer password (e.g. up to 12 characters) including alphabet, numerical and special character as a first or second protection layer before using Biometric;

iii. When setting and activating Biometric for the first time, the customer should be authenticated with a combination of other forms of multi-factor authentication.

iv. When Biometric data is required to be stored by the FIs (e.g. MFM, Kiosk), FIs should safeguard individual's Biometric such as ensuring the Biometric data is encrypted and stored in a highly-protected database;

v. When Biometric data is compared with other database (e.g. customer device, third party), the original Biometrics should only be limited for comparison purposes and should not be copied to the FIs system;

vi. FIs to regularly update and patch its software or application that captures and verifies Biometrics; and

vii. FIs should only enable individual to use Biometric on registered devices.

9.13.4 FIs that offer verification and confirmation of payment or other service transaction via Biometric technology specifically at merchant level should consider the following:

i. Assess suitability of the Biometric to be used, whether fingerprint, iris or voice recognition based on the risks and performance;

ii. FIs should regularly maintain and upgrade the application that capture and verifies the Biometric;

iii. FIs should rely on more than one type of identification for this purpose; and

iv. FIs should provide an alternative method in the event payment via Biometric technology is inaccessible or inoperable.

9.14 Quick Response (QR) Code

9.14.1 The use of a QR Code potentially provides convenience to both FIs and customers as well as the merchant, as QR codes can be used as an alternative form of payment facility or to access service efficiently. However, FIs should be mindful of the use of suspicious, fake or invalid QR Code that may affect the service delivery.

9.14.2 FIs that provide QR Codes whether for the purpose of customers to get more information on its product offering, payment or survey, the following measures should be considered:

i. QR Code at participating merchant – FIs should ensure the static QR Code displayed by merchant is genuine and a special feature or logo of the FIs is visible for customer to confirm it is a legitimate QR Code;

ii. FIs should maintain a list of participating merchants that uses QR Codes for the purpose of payment;

iii. FIs should regularly conduct a review on all its participating merchant to ensure the QR Code is not tampered or falsified; and

iv. QR Code in newspaper, website or digital media – FIs should ensure the QR Code provided is genuine and to also include a link underneath the QR Code as an alternative.

9.14.3 FIs should ensure the QR Code will directly link to the intended webpage or digital services. It is recommended that the QR Code is to be generated by the FIs' application. If a third party QR code generator is used, the FIs should ensure the third party will not collect data when customer scanned on the QR code.

9.15 Near-Field-Communication (NFC)

9.15.1 In the context of Digital Financial Services using NFC method, this refers to FIs that offer contactless transaction either by using the customer's payment cards, e-Wallet, mobile application or smart device (such as smartwatch or smart wristband). However, as the reader and payment devices must be brought into close proximity with each other in order to complete the contactless payment, FIs should be mindful of the risks relating to skimming, eavesdropping, interception attacks, theft and loss of device.

9.15.2 In view of such risks, the following security measures should be considered:

i. FIs to use secured channels to make payments. Secure channels encrypt data so only authorised device can decode it;

ii. FIs to regularly maintain and update its devices whether at application level or reader device;

iii. FIs to inform and provide clear information to the customers of their responsibility in the event of theft or loss of card or device. Customers should also be advised to immediately notify the FIs for the FIs' further action to minimise the risk of financial loses;

iv. FIs to disable option for NFC at application level and disable "reader device to remain active when not in use" to prevent active-active pairing;

v. For payment using NFC feature, FIs should request additional authentication either by using Biometric, signature or PIN for high-value transactions; and

vi. Regardless of the value of transactions, payment using NFC feature should be recorded in the system as usage or transaction history.

9.15.3 FIs should ensure their merchants only use authorised reader devices provided by the FIs. As such, FIs should regularly conduct review on the participating merchant to avoid tampered or unauthorised reader device.

9.15.4 In the case when merchants use their own NFC-enabled device, the FIs should establish minimum technical requirements and security configuration for device that can be used.

9.16 Digital Signature

9.16.1 In an online platform, signing forms or agreements for digital financial services may use digital signature. The FIs should assess the suitability of using digital signature and determine if there are special legal and regulatory requirements relating to signing of certain documentation.

9.16.2 Digital signature should be in the form of the following:

i. When the customer logs in using their own user account and submits the form via online application or portal, this can be considered as digitally signed. However, the FIs should add statements on the form to clarify that upon submitting the form, the user has expressed their commitment to the service. Optionally, the FIs may also use a checkbox or require additional login to reinforce the signing.

ii. The FIs may use certificate-based digital signature to sign softcopy of document or online form. This certificate-based digital signature should be based on the FIs' cryptography standard covered in Paragraph 7.4 on Cryptography. FIs should be able to provide the customer with necessary tools for the digital signing or ensure that these tools are easily available.

9.16.3 The digitally signed data, form or document should be sent over a secure channel that allows the FIs to confirm the identity of customer such as ensuring the user account and e-mail address used to send the digitally signed data, form or document is the same as in the digital signature details.

9.16.4 When using digital signature for digital financial services, the FIs should ensure that the digital signing process for making consent are made clear to the customer and agreed by both parties.

9.17 Other Digital Financial Services

9.17.1 With the advancement in technology, FIs should exercise caution and remain proactive in identifying emerging technology and new cyber threats that may be disruptive to their business. It is always expected for FIs to conduct risk assessment and analysis whether its current infrastructure and employee's capability are able to manage, control and contain technological threats when introducing new technology or feature into its current business.

9.17.2 For any products or services that uses other form of technology that are not described above, FIs should prepare the following:

i. Rationale on the proposal;

ii. Risk assessment and analysis on the new technology and business process;

iii. Strategic roadmap including timeline to address concerns identified after risk assessment and analysis;

iv. End-to-end process flow; and

v. Architecture diagram and/or data-flow diagram that will help to explain the interrelationship between FIs applications/modules/components.

9.17.3 The FIs should ensure that the new digital financial services are within the allowed services or activities for the FIs' license type and legislations relevant to their licenses. The FIs should also be able to demonstrate that the offering of digital financial services will not diminish the FIs' capability to comply with the relevant legislations.

9.17.4 For innovative digital solutions that have the potential to introduce new types of financial products or services, it is recommended for the FIs to experiment and test the product or services before rolling out to the public. The FIs may consider leveraging BDCB's FinTech Regulatory Sandbox for the experimentation.

10. CONSUMER PROTECTION

While offering product and services to the financial consumers, it is important for FIs to also protect consumer's interests in order to maintain trust. It is undeniable that consumer personal data are vital in businesses and generate opportunities for FIs in transforming their businesses. However, FIs should be mindful of the ethics and relevant law relating to consumer protection and market conduct.

10.1 Consumer Personal Data Protection

10.1.1 When it is necessary to collect customer's personal data, the FIs should clearly indicate the purpose of the data collection and have in place a suitable method to obtain consent from the customer.

10.1.2 Data protection or privacy policy should be established or to be included in the terms and conditions, and made available to the customer.

10.1.3 FIs should communicate any changes to the privacy policy or terms and conditions, and to request for renewed consent if the changes affect data protection and privacy policy.

10.1.4 Any major changes to the FIs' customer-facing system especially changes to data structure or data input field should be communicated to the customers such as in version history list or release notes.

10.1.5 When there are changes that require additional consent, negative consent method should not be used. The FIs should follow up with the customer to obtain the consent.

10.1.6 FIs should not gain consent through force or unsolicited way. Instead, the FIs may communicate the consequences or limitations on the FIs' side if the FIs are unable to obtain necessary consent to the customer's personal information.

10.1.7 FIs should also provide clear disclaimers if their customer-facing system automatically collects data such as via cookies or data analytic tool.

10.1.8 FIs should ensure their customer personal data are accurate, current and complete. The FIs should establish relevant process to request or allow customers to review and update their personal data.

10.1.9 The FIs should be able to demonstrate that the storage of customer personal data is secure and when required, to clearly indicate the controls in place to the customers.

10.1.10 When sending over customer personal information such as bank statement or payment receipt online, the FIs should arrange adequate protection such as encryption to protect the data from unauthorised receiver.

10.1.11 The FIs should establish relevant processes to handle customers request for information on how the FIs have been using their personal data over certain period of time, and in the event the customers withdraw their consent.

10.1.12 The FIs should ensure that customer personal data can be tracked such as using homogeneous data structure, or at least can be traced through system audit trail, database logs and file version history.

10.1.13 FIs should review the purpose of customer personal data and ensure the use of the personal data remains relevant to the consented purpose, especially when there are changes to the FIs systems or processes that can affect the customer's personal data.

10.1.14 If the customer personal data has to be stored on a cloud platform or other third party, such arrangement including country where the customer's personal data is stored should be informed to the customer. Access to the customer personal data should be restricted.

10.1.15 If the FIs have to assign a third party to process customer personal data, the FIs should inform the customer on this arrangement and to limit access to personal data such by using pseudonymisation technique or encryption.

10.1.16 FIs should also be mindful of any applicable statutory or regulatory requirements on data retention, that may include retention of customer personal data. Where necessary, these requirements should be communicated to the customer.

10.2 Customer Account Management

10.2.1 When customer is provided with access to FIs' system such as service portal or mobile application, user access management is applicable on the customers, which includes the following:

i. Customers should only be assigned with minimal access suitable for customers to perform relevant financial services, enquiries and requests;

ii. The customer's user account should only be able to manage services and products that are associated with the customer;

iii. Customers should not have access to other customer's accounts unless joint or linked accounts. In such cases, there should be controls to limit certain activities. For example, for credit card, supplementary card holder should have less access than the principal card holder;

iv. Customers' accounts are governed by a formally defined process covering the creation, modification, maintenance and deletion of accounts;

v. Customer user accounts should be uniquely identifiable and their login activities should be recorded; and

vi. Enforce strong password and recommend periodic password change, unless multi-factor authentication is used to support the password.

10.2.2 Customer user accounts should also be reviewed to detect inactive or dormant user accounts and there should be process in place to manage these inactive or dormant user accounts.

10.2.3 The FIs should provide user account management page that allow the customer to view, update and manage their user account details and profiles.

10.2.4 Multifactor authentication is highly recommended for user accounts that involve payment and sensitive information. The FIs should offer and encourage customers to use multifactor authentication.

10.2.5 To reduce misuse and improper use of customer user account, the FIs should provide put in place terms of use for customer user account that outlines customer's responsibility and acceptable use.

10.2.6 The FIs should also provide education and awareness to the customers on good practice to protect their user account that consider following:

i. Change their password every six months at the very minimum and increase the complexity of their password;

ii. Not to share their user account and sensitive information to others;

iii. Remind customers that the FIs will not ask for user account's password or multifactor authentication details through social networking sites, email or phone unless secure communication platform is available;

iv. Frequently review their account information and user access;

v. To log out their user account once they have completed their online transactions; and

vi. To timely inform the FIs for any suspicious activity on their account.

10.2.7 In addition to login page, online registration page should also be secured and the data submitted should be protected with encryption such as SSL or TLS.

10.2.8 FIs should ensure there are reliable and secure processes and methods in place in providing or delivering customer account details to the customers.

10.3 Customer Awareness

10.3.1 FIs should provide adequate security awareness to their customers that educates them on how to securely conduct their online and electronic transactions via the FIs' systems as well as recommending security measures and providing guidelines to mitigate or reduce any technology risks.

10.3.2 FIs can deliver awareness materials to their customers by using but not limited to the following methods:

i. Official website;

ii. Application login page;

iii. Booklets, pamphlets and posters that are available at their branches;

iv. Email;

v. Social media;

vi. Short Message System (SMS);

vii. Briefing their customers during the registration of their online services; and

viii. Awareness program such as kiosk or booth during events.

10.3.3 Written instructions and guidelines on the use of the FIs' system and digital financial services should be adequately provided during the customer registration and made available on the FIs' available platform such as website.

10.3.4 The customer security awareness program should be also be updated and disseminated regularly when there are new features and security requirements on any of their online and electronic services.

10.3.5 FIs should remind their customers on the need to protect their personal details and other confidential data. Customers need to secure their PINs, security tokens and mobile phones which contain their digital financial services application, and any other devices (computer, laptops, tablets) used to access their digital financial services.

10.3.6 FIs should provide customers with clear instructions on what to do or who to contact in the event customers have suspicions that their account has been compromised, or there are fraudulent activities in their account.

10.4 Transaction and Fraud Monitoring

10.4.1 FIs should put in place a system to monitor transactions for fraudulent activities. The FIs' system should have the capability to store and retain information or logs of such activities.

10.4.2 The storage of such information or logs should be secure and the integrity of the information should be protected.

10.4.3 The monitoring system should be reviewed, maintained and updated to ensure the monitoring remain effective.

10.5 Customer Issue Reporting and Support

10.5.1 FI should determine appropriate channel and establish process for customers to report application issues, to make query or request relating to the application and/or digital financial services.

10.5.2 Customer queries and complaints relating to digital financial services should be recorded and compiled. This information should be analysed in planning new features, application improvement, bug fixes and problem management.

10.5.3 FIs that collect customer's personal data and usage data for analytic purpose, regardless anonymous or not, should observe Paragraph 10.1 on Consumer Personal Data Protection.

MANAGING DIRECTOR
BRUNEI DARUSSALAM CENTRAL BANK

Issue Date: 16 Jamadilakhir 1443H / 20 January 2022M