BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Risk Management in Technology (RMiT)

Applicable to:
1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed insurers including professional reinsurers
5. Licensed takaful operators including professional retakaful operators
6. Prescribed development financial institutions
7. Approved issuers of electronic money
8. Operator of a designated payment system
9. Registered merchant acquirers
10. Intermediary remittance institutions

Issued on: 28 November 2025 BNM/RH/PD 028-98

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 With the prevalent use of technology in the provision of financial services, financial institutions must-

(a) invest in the required expertise and risk controls to prevent operational disruptions given the complexity of Information Technology (IT) systems;
(b) achieve the highest level of security to combat fast-changing digital crimes for public confidence;
(c) maintain robust oversight to prevent transmission of risks with increased third party interlinkages;
(d) build operational resilience against sophisticated and malicious cyber threats amidst heightened cyber risks globally; and
(e) practice ethical and responsible use of technology for inclusive growth.

1.2 This policy document sets out the Bank's policy objectives and minimum requirements to improve financial institutions' management of technology risk, including cyber risk. In applying this policy document, a financial institution shall have regard to the size and complexity of its operations, the level of technology use and its external stress exposure. Accordingly, larger and more complex financial institutions, or those with a high degree of digitalisation and linkages with third parties, are required to adopt more robust risk controls that commensurate with the increased technology risk exposure of the institution.

1.3 Enforcement or supervisory actions can be taken against the financial institutions including its directors, officers and employees for any non-compliance with any provision marked as "S" in Part B of this policy document.

1.4 Where the Bank considers that a financial institution's technology risk management has material weaknesses which, if not promptly and effectively addressed, might contribute to, or result in, non-compliance with this policy document, the Bank may, among others-

(a) require an independent external review of the overall or specific areas of the financial institution's technology risk management;
(b) require the financial institution to develop and implement specific remediation plan;
(c) require the financial institution to hold additional capital; or
(d) require the financial institution to take any other corrective action necessary to rectify the weaknesses in a sustainable manner.

2 Applicability

2.1 Subject to paragraph 2.2, this policy document is applicable to all financial institutions as defined in paragraph 5.2.

2.2 The following paragraphs and appendices are not applicable to certain financial institutions identified below:

(a) Part C (paragraphs 16 to 17) and **Appendices 6 and 7** are not applicable to-
  (i) operators of designated payment system;
  (ii) eligible e-money issuers;

(iii) non-bank registered merchant acquirers; and
(iv) intermediary remittance institutions; and

(b) paragraphs 12.3 to 12.9 are not applicable to-
(i) operators of designated payment system; and
(ii) intermediary remittance institutions; and

(c) paragraph 13.3 is not applicable to the following financial institutions, provided they have not been designated as National Critical Information Infrastructure (NCII) entities[1]:
(i) eligible e-money issuers;
(ii) non-bank registered merchant acquirers; and
(iii) intermediary remittance institutions.

3 Legal provisions

3.1 The requirements in this policy document are specified pursuant to-
(a) sections 47(1), 47(2)(d) and 143(2) of the Financial Services Act 2013 (FSA);
(b) sections 57(1), 57(2)(d) and 155(2) of the Islamic Financial Services Act 2013 (IFSA);
(c) sections 41(1), 41(2)(b) and 116(1) of the Development Financial Institutions Act 2002 (DFIA); and
(d) sections 34(2) and 74 of the Money Services Business Act 2011 (MSBA).

3.2 The guidance in this policy document is issued pursuant to section 266 of the FSA, section 277 of the IFSA, section 126 of the DFIA and section 74 of the MSBA.

4 Effective date

4.1 This policy document comes into effect on 28 November 2025 except where otherwise stated explicitly in this policy document.

5 Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, IFSA, DFIA or MSBA, as the case may be, unless otherwise defined in this policy document.

5.2 For purposes of this policy document-

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action;

"G" denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted;

[1] For clarity, this refers to financial institutions that have not been designated as NCII entities by BNM under subsection 17(1) of the Cyber Security Act 2024, which came into effect on 26 August 2024.

"affiliate" in relation to an entity, refers to any corporation that controls, is controlled by, or is under common control with, the entity;

"board" refers to the board of directors of a financial institution, including any committee carrying out any of the responsibilities of the board under this policy document;

"critical system" refers to any application system that supports the provision of critical banking, insurance, takaful, payment, investment or trading services, where failure of the system has the potential to significantly impair the financial institution's provision of financial services to customers or counterparties, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements;

"customer and counterparty information" refers to any information relating to the affairs or the account, of any customer or counterparty of a financial institution in whatever form;

"cyber incident" refers to a cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not;

"cyber resilience" refers to the ability of people, processes, IT systems, applications, platforms or infrastructures to withstand adverse cyber events;

"digital services" refers to the provision of payment, remittance, banking, Islamic banking, insurance or takaful services delivered to customers via electronic channels and devices including Internet and mobile devices, self-service and point-of-sale terminals;

"disruption" refers to an incident that causes degradation to the normal performance of a business function that would affect a financial institution's ability to continue its operations and services to its customers;

"financial institution" refers to-

(a) a licensed person under the FSA and the IFSA (excluding branches of a foreign professional reinsurer and a professional retakaful operator);
(b) a prescribed institution under the DFIA;
(c) an eligible e-money issuer as defined[2] in the policy document on Electronic Money issued on 31 January 2025[3];
(d) an operator of a designated payment system under the FSA and IFSA;
(e) a non-bank registered merchant acquirer as defined[4] in the policy document on Merchant Acquiring Services issued on 15 September

[2] For ease of reference, an "eligible e-money issuer" is defined as an approved issuer of electronic money with substantial market presence based on the criteria set out in **Appendix 1** of the policy document on Electronic Money or such other criteria as may be specified by the Bank from time to time.
[3] Including any amendments or modifications made after the issuance date.
[4] For ease of reference, a "non-bank registered merchant acquirer" refers to any person who is registered pursuant to sections 17(1) and 18 of the FSA to provide merchant acquiring services and fulfils the criteria under paragraph 2.1 of the policy document on Merchant Acquiring Services or such other criteria as may be specified by the Bank from time to time but does not include a licensed bank, licensed Islamic bank or prescribed institution.

2021[5], with a market share of at least 5% of the total non-bank merchant acquiring services transaction value or volume in Malaysia for a given year; and

(f) an intermediary remittance institution (IRI) as defined[6] in the policy document on Governance, Risk Management, and Operations for Money Services Business (MSB) issued on 9 April 2025[7], with a market share of at least 5% of total IRI transaction value or volume in Malaysia for a given year;

"OTP or one-time password" refers to an alphanumeric or numeric code represented by a minimum of 6 characters or digits which is valid only for single use;

"senior management" refers to the Chief Executive Officer and senior officers, who are employed by a financial institution or an affiliate of the financial institution. This includes, at minimum, senior management roles listed in Appendix 2 of policy document of Responsibility Mapping issued on 29 December 2023 as well as the relevant paragraphs on roles and responsibilities in the policy documents[8] on Electronic Money issued on 31 January 2025, Merchant Acquiring Services issued on 15 September 2021, Payment System Operator issued on 22 December 2022, and Governance, Risk Management, and Operations for Money Services Business (MSB) issued on 9 April 2025;

"third party service provider" refers to any internal group affiliate or external entity providing technology-related functions or services directly to enable or support a function or service provided by the financial institution, or which involves the transmission, processing, storage or handling of confidential information pertaining to the financial institution or its customers. This includes cloud computing software, platform and infrastructure service providers.

6 Related legal instruments and policy documents

6.1 This policy document must be read together with any relevant legal instruments, policy documents, guidelines, circulars, and supplementary documents issued by the Bank, including any amendments and reissuances thereafter, in particular-

(a) Guidelines on Data Management and MIS Framework issued on 23 October 2008;
(b) Guidelines on Data Management and MIS Framework for Development Financial Institutions issued on 5 November 2012;
(c) Policy Document on Risk Governance issued on 1 March 2013;
(d) Policy Document on Introduction of New Products issued on 7 March 2014;
(e) Policy Document on Compliance issued on 10 May 2016;

[5] Including any amendments or modifications made after the issuance date.
[6] For ease of reference, an "intermediary remittance institution or IRI" refers to an intermediary institution that receives wire transfers on behalf of a sending remittance company, for onward transmission, to a receiving party that will then disburse to the beneficiary of the wire transfer as may be specified by the Bank from time to time.
[7] Including any amendments or modifications made after the issuance date.
[8] Including any amendments or modifications made after the issuance date for the referenced policy documents.

(f) Policy Document on Operational Risk issued on 10 May 2016;
(g) Policy Document on Debit Card and Debit Card-i issued on 2 December 2016;
(h) Policy Document on Credit Card and Credit Card-i issued on 2 July 2019;
(i) Policy Document on Outsourcing issued on 23 October 2019;
(j) Policy Document on Interoperable Credit Transfer Framework issued on 23 December 2019;
(k) Policy Document on Merchant Acquiring Services issued on 15 September 2021;
(l) Circular of Notification on Consolidated List of Requirements Relating to Technology and Cyber Risk issued on 29 September 2022;
(m) Policy Document on Business Continuity Management issued on 19 December 2022;
(n) Policy Document on Responsibility Mapping issued on 29 December 2023;
(o) Industry letter on Updated 2023 Financial Stability Board Cyber Lexicon issued on 28 February 2024;
(p) Policy Document on Fair Treatment of Financial Consumers issued on 27 March 2024;
(q) Specifications on Countermeasures to Combat E-Money Fraud issued on 8 April 2024;
(r) Policy Document on Operational Risk Reporting issued on 10 April 2025; and
(s) Management of Customer Information and Permitted Disclosures (MCIPD) issued on 31 October 2025.

7 Policy documents and circulars superseded

7.1 This policy document supersedes the following policy documents, guidelines, circulars and notifications:
(a) Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions, including for the provisions under paragraphs 21, 22 and 26 issued on 18 November 2019;
(b) Specifications on Measures to Combat Electronic Banking Fraud dated 23 August 2022;
(c) Measures to Combat Fraud Monetised via Internet Banking and Mobile Banking dated 31 May 2022;
(d) Policy Document on Risk Management in Technology (RMiT) issued on 1 June 2023;
(e) Additional Guidance on Technology and Cyber Safeguards to Ensure the Protection of Customer Information issued on 10 July 2023; and
(f) Specifications on Fraud Detection Standard dated 27 March 2024.

PART B POLICY REQUIREMENTS

8 Governance

Responsibilities of the Board of Directors

S 8.1 The board must establish and approve the technology risk appetite which is aligned with the financial institution's risk appetite statement. In doing so, the board must-

(a) approve the corresponding risk tolerances for technology-related events considering potential impact on business operations as well as its customers;
(b) identify risk owner to ensure clear accountability and establish criteria and approving authority for the acceptance of residual risks by the institution;
(c) ensure key risk indicators are identified to monitor existing and emerging risks against financial institution's risk tolerance;
(d) ensure sufficiency and appropriate deployment of resources; and
(e) conduct review of the technology risk appetite at regular intervals with sufficient deliberation to ensure such risk appetite remains relevant with changing risk environment.

S 8.2 In discharging its oversight responsibility, the board must-

(a) approve and review the adequacy of the financial institution's IT and cybersecurity strategic plans to meet business objectives covering a period of no less than three years;
(b) endorse and oversee the effective implementation of a sound and robust technology risk management framework (TRMF) and cyber resilience framework (CRF), as required to be developed under paragraphs 9.1 and 11.2, for the continuity of operations and delivery of financial services;
(c) require senior management to continuously demonstrate that risk assessments undertaken in relation to critical IT systems and use of emerging technology are robust and comprehensive, supported with adequate control measures and resources to mitigate IT and cyber risks arising from the execution of IT strategic plans;
(d) ensure IT-related framework, policies and guidelines are reviewed at least once every three years (unless otherwise stated in this policy document) and apply a depth of review that is commensurate with the complexity of the financial institution's operations and changes in the risk environment; and
(e) ensure risk management framework provide support to robust risk assessments in relation to technology related applications submitted to the Bank.

S 8.3 The board must designate a board-level committee[9] which shall be responsible for supporting the board in providing oversight over technology-related matters. The composition of the designated committee must include

[9] The board of a financial institution may either designate an existing board committee or establish a separate committee for this purpose. Where such a committee is separate from the Board Risk Committee (BRC), there must be appropriate interface between this committee and the BRC on technology risk-related matters to ensure effective oversight of all risks at the enterprise level.

at least one member with technology experience and competencies.

S 8.4 To promote effective discussion at the board level amidst a rapidly evolving technology and cyber risk landscape, the board must-

(a) obtain regular updates on technology risk and cyber threats;
(b) allocate sufficient time to discuss cyber risks, including the strategic, reputational and liquidity risks and impact of operational disruption to stakeholders which could arise from an extreme cyber incident. This shall be supported by input from external experts where appropriate; and
(c) participate in relevant cybersecurity awareness and training programmes.

S 8.5 The board audit committee (BAC) shall be responsible for ensuring the effectiveness of the internal technology audit function. This shall include ensuring the adequate competence of the audit staff to perform technology audits. The BAC shall review and ensure appropriate audit scope, procedures and frequency of technology audits. The BAC shall also ensure effective oversight over the prompt closure of corrective actions to address technology control gaps.

Responsibilities of the senior management

S 8.6 The senior management shall bear primary responsibility for the day-to-day management of technology risks including cyber risks. In fulfilling its responsibilities, senior management must–

(a) implement board approved TRMF and CRF into specific policies and procedures that are consistent with the approved risk appetite and risk tolerance;
(b) ensure that the crisis management plan for service disruptions provides for timely escalation of recovery action, taking into consideration the impact on customers, such as:
    (i) duration of disruption;
    (ii) number of customers affected by a disruption; and
    (iii) number and value of financial transaction impacted; and
(c) provide regular updates to the board on the status of key performance indicators with pertinent information on the risk controls to facilitate informed performance review.

S 8.7 The senior management must establish a cross-functional committee to provide guidance on the financial institution's technology plans and operations. The members of the committee must include senior management from both cyber and technology functions, as well as major business units. The committee's responsibilities shall include the following:

(a) oversee the formulation and effective implementation of the strategic technology plan and associated technology policies and procedures;
(b) provide timely updates to the board on key technology matters[10]; and

[10] Key technology matters include updates on critical systems' performance, significant IT and cyber incidents, management of technology obsolescence risk, status of patch deployment activities for critical technology infrastructure, proposals for and progress of strategic technology projects, performance of critical technology outsourcing activities, utilisation of the technology budget and competencies for managing technology risks.

(c) approve any deviation from technology-related policies after having carefully considered a robust assessment of related risks. Material deviations shall be reported to the board.

The rest of the page is intentionally left as blank

9 Technology Risk Management

Risk Management Framework

S 9.1 A financial institution must ensure that the TRMF is an integral part of the financial institution's enterprise risk management framework (ERM).

S 9.2 The TRMF must include the following:

(a) clear definition of technology risk;
(b) clear responsibilities assigned for the management of technology risk at different levels and across functions, with appropriate governance and reporting arrangements;
(c) the identification of technology risks to which the financial institution is exposed, including risks from the adoption of new or emerging technology (refer **Appendix 9** on Guidance on Emerging Technologies);
(d) risk classification of all information assets / systems based on its criticality;
(e) risk measurement and assessment approaches and methodologies;
(f) risk controls and mitigations;
(g) continuous monitoring to timely detect and address any material risks;
(h) effective information system to ensure the technology risk profile remains accurate and up to date;
(i) identification of key resources and interdependencies (including critical third party service providers and their connected parties[11]) which support delivery of critical technology functions;
(j) undertake scenario analysis to strengthen capacity and readiness to resume critical systems under severe conditions; and
(k) effective incident management policies and procedures to minimise the impact of any service disruption on the financial institution and its customers, by restoring the affected service or system to a secure and stable state as quickly as possible.

S 9.3 A financial institution must establish an independent enterprise-wide technology risk management function which is responsible for-

(a) implementing the TRMF and CRF;
(b) advising on critical technology projects and ensuring critical issues that may have an impact on the financial institution's risk tolerance are adequately deliberated or escalated in a timely manner; and
(c) providing independent views to the board and senior management on third party assessments[12], where necessary.

[11] Connected parties refers to Nth party as defined by Basel Committee on Banking Supervision on principles for the sound management of third party risk.
[12] Relevant third party assessments may include the Data Centre Resilience and Risk Assessment, Network Resilience and Risk Assessment and independent assurance for introduction of new or enhanced digital services.

Designated Chief Information Security Officer

S 9.4 A financial institution must designate a Chief Information Security Officer[13] (CISO) by whatever name called, to be responsible for the technology risk management function of the financial institution. The financial institution must ensure that the CISO has sufficient authority, independence and resources[14]. The CISO shall-

(a) be independent from day-to-day technology operations;
(b) apprise board and senior management of current and emerging technology risks which could potentially affect the financial institution's risk profile;
(c) have the requisite technical skills in emerging and core technologies used by the institution, expertise and experience in audit, governance and risk management, strategic planning and execution of IT and cybersecurity programs, and third party risk management; and
(d) be appropriately certified.

S 9.5 The CISO shall be responsible for ensuring that the financial institution's information assets and technologies are adequately protected, which includes-

(a) formulating appropriate policies for the effective implementation of TRMF and CRF;
(b) enforcing compliance with these policies, frameworks and other technology-related regulatory requirements; and
(c) advising senior management on technology risk and security matters, including developments in the financial institution's technology security risk profile in relation to its business and operations.

[13] In line with the role defined in Responsibility Mapping policy document dated 29 December 2023, including any amendments or modifications made after the issuance date.

[14] A financial institution's CISO may take guidance from the expertise of a group-level CISO, in or outside of Malaysia, and may also hold other roles and responsibilities provided these do not impair the CISO's independence or competence. Such designated CISO shall be accountable for and serve as the point of contact with the Bank on the financial institution's technology-related matters, including managing entity-specific risks, supporting prompt incident response and reporting to the financial institution's board.

10 Technology Operations Management

Technology Project Management

S 10.1 A financial institution must establish appropriate governance requirements commensurate with the risk and complexity[15] of technology projects undertaken. This shall include project oversight roles and responsibilities, authority and reporting structures, and risk assessments throughout the project life cycle.

S 10.2 The risk assessments shall identify and address the key risks arising from the implementation of technology projects. These include the risks that could threaten successful project implementation and the risks that a project failure will lead to a broader impact on the financial institution's operational capabilities. At a minimum, due regard shall be given to the following areas:

(a) the adequacy and competency of resources including those of the vendor to effectively implement the project. This shall also take into consideration the number, size and duration of significant technology projects already undertaken concurrently by the financial institution;
(b) the complexity of systems to be implemented such as the use of unproven or unfamiliar technology and the corresponding risks of integrating the new technology into existing systems, managing multiple vendor-proprietary technologies, large-scale data migration or cleansing efforts and extensive system customisation;
(c) the adequacy and configuration of security controls throughout the project life cycle to mitigate cybersecurity breaches or exposure of confidential data;
(d) the comprehensiveness of the user requirement specifications to mitigate risks from extensive changes in project scope or deficiencies in meeting business needs;
(e) the robustness of system and user testing strategies to reduce risks of undiscovered system faults and functionality errors;
(f) the appropriateness of system deployment and fallback strategies to mitigate risks from prolonged system stability issues; and
(g) the adequacy of disaster recovery operational readiness following the implementation of new or enhanced systems.

S 10.3 The board and senior management must receive and review timely reports on the management of these risks on an ongoing basis throughout the implementation of significant projects.

[15] For example, large-scale integration projects or those involving critical systems must be subject to more stringent project governance requirements such as more frequent reporting to the board and senior management, more experienced project managers and sponsors, more frequent milestone reviews and independent quality assurance at major project approval stages.

System Development and Acquisition

S 10.4 A financial institution must establish a framework to guide the design, planning, implementation, and governance of an enterprise technology architecture. A technology architecture serves as a foundation on which financial institutions plan and structure system development and acquisition strategies to meet business goals. Thus, the financial institution must ensure the framework carry out these functions-

(a) provides a comprehensive view of technology throughout the financial institution, baseline architecture components and key rationale for their use;

(b) is an overall technical design and high-level plan that describes the financial institution's technology infrastructure, systems' inter-connectivity and dependencies (e.g. fallback facility), and security controls. The outlined information is critical to support identification of a single point of failure;

(c) contains mapping to supported business functions, organisation units, applications, and data to enable business impact analysis;

(d) defines principles and guideline to govern the design and maintenance of the network infrastructure, related technology controls, and IT security policies; and

(e) outline longer-term priorities to guide its evolution.

S 10.5 A financial institution must adopt a methodology for an effective and secure implementation of IT systems. Key phases of System Development Life Cycle (SDLC) shall include requirement, design, development, testing, deployment, change management, maintenance and decommissioning, and integrate with-

(a) enterprise architecture to ensure successful execution of business strategy;

(b) risk management policies and practices to achieve business objectives; and

(c) security principles[16] and requirements to ensure confidentiality, integrity, and availability of customer and counterparty information.

S 10.6 A financial institution must meet enterprise security, governance and compliance requirements when using rapid system development methodology[17]. Given the dynamic environment can increase likelihood of errors, a financial institution shall automate the IT security compliance review to prevent unauthorised access as well as the discovery and testing of security vulnerabilities to ensure secure release of new IT services.

[16] The security considerations shall include ensuring appropriate segregation of duties throughout the SDLC.

[17] Such as DevOps which is a set of practices for automating the processes between software development and information technology operations teams so that they can build, test, and release software faster and more reliably. The goal is to shorten the systems development life cycle and improve reliability while delivering features, fixes, and updates frequently in close alignment with business objectives.

S 10.7 A financial institution shall physically segregate the production environment from the development and testing environment to mitigate the risk of unauthorised changes to the production systems. Where a financial institution is relying on a cloud environment, the financial institution shall ensure that these environments are not running on the same virtual host.

S 10.8 A financial institution must establish a sound methodology for a rigorous system testing prior to deployment. The testing shall ensure that the system meets user requirements and performs robustly. Where sensitive test data is used, the financial institution must ensure proper authorisation procedures and adequate measures to prevent their unauthorised disclosure are in place.

G 10.9 The scope of system testing referred to in paragraph 10.8 may include unit testing, integration testing, user acceptance testing, application security testing, stress and load testing, regression, exception and negative testing, where applicable.

S 10.10 A financial institution must ensure any changes to the source code of critical systems are subject to adequate source code reviews to ensure code is secure and developed in line with recognised coding practices prior to introducing any system changes.

S 10.11 A financial institution must establish appropriate procedures to independently review and approve system changes. The financial institution must also establish and test contingency plans in the event of an unsuccessful implementation of material changes to minimise any business disruption.

S 10.12 In relation to critical systems that are developed or maintained by third party service provider, a financial institution must, through contractual obligations, require third party service provider to:

(a) provide sufficient notice to the financial institution before any changes are undertaken that may impact the IT system;
(b) demonstrate that it adopts secure by design principles in IT system development methodology to mitigate cyber risks from propagating across the supply chain; and
(c) ensure the source code continues to be readily accessible for business continuity.

S 10.13 When decommissioning critical systems, a financial institution must ensure minimal adverse impact on customers and business operations. This includes establishing and testing contingency plans in the event of unsuccessful system decommissioning.

G 10.14 A financial institution may deploy automated tools for software development, testing, software deployment, change management, code scanning and software version control to facilitate timely security assessment of critical systems in keeping with growing complexity in IT systems and emerging cyber threats.

G 10.15 Where a third party software is used, a financial institution should consider the potential risks and impacts a cyber supply chain incident may pose to its overall business operations and services. A financial institution may consider-

(a) adopting Software-Bill-of-Materials (SBOM)[18] to automate the identification and continuous monitoring of potential security vulnerabilities including security issues associated with third party software components; and

(b) establishing open-source software security policy and procedures. This includes ensuring secure access to source code repositories in third party platforms, regular monitoring to prevent data leakages, adoption of secure coding practices, robust testing of open-source software and timely vulnerability assessment to mitigate security vulnerabilities and propagation of malwares across supply chain.

S 10.16 A financial institution must develop and implement robust policies to identify and reduce shadow IT[19] risks.

Patch and End-of-Life System Management

S 10.17 A financial institution must ensure that all systems including digital services are not running with known security vulnerabilities[20], on outdated platform or end-of-life (EOL) technology systems. In this regard, a financial institution must-

(a) maintain current security baseline for the security hardening of technology components and ensure the security baseline is accurate and up to date;

(b) continuously monitor and implement latest patch releases in a timely manner;

(c) identify, plan and implement remedial action for technology systems that are approaching EOL; and

(d) obtain management approval for any exception permitting the continued use of unsupported or outdated technology. This exception must be substantiated by a thorough risk assessment with clear timeline for phasing out the outdated technology and are regularly reviewed at least on annual basis to ensure associated risks are effectively managed.

[18] Software-Bill-of-Materials (SBOM) refers to a formal record containing the details, and the various components used in building a software product including its related supply chain relationships. SBOM provides increased transparency, provenance, and speed at which vulnerabilities can be identified and remediated across the SDLC.

[19] Shadow IT refers to unauthorised use of hardware, software, or other systems and services within a company, commonly without the IT department's approval, knowledge, or oversight.

[20] Known security vulnerability refers to a documented flaw or weakness in a system that are publicly disclosed or catalogued in databases such as the National Vulnerability Database (NVD) or Common Vulnerabilities and Exposures (CVE) list.

S 10.18 A financial institution must establish a patch and EOL management framework which addresses among others the following requirements:
(a) identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems;
(b) formulation of criteria, priority and turnaround time for patch deployment according to the severity of the vulnerabilities identified;
(c) conduct of compatibility testing prior to the deployment of patches to minimise disruption to connected systems;
(d) adherence to the workflow for end-to-end patch deployment processes including approval, testing, monitoring and tracking of activities; and
(e) end-user awareness for orderly transition.

S 10.19 A financial institution must continually monitor the effectiveness and security of the technology in use, incorporating developments in technology that may disrupt existing security controls[21]. A financial institution shall-
(a) ensure its board receives advice on the potential impact to business operation arising from evolving technology landscape;
(b) formulate long-term strategy to address anticipated changes with allocation of competent resources to manage associated risks, including new cyber adversary tactics and techniques; and
(c) establish roadmap for system migration to preserve security and reliability of the technology infrastructure in an orderly manner.

Cryptography

S 10.20 A financial institution must establish a robust and resilient cryptography policy to promote the adoption of strong cryptographic controls for protection of important data and information. This policy, at a minimum, shall address requirements for-
(a) the adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;
(b) the adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction;
(c) the periodic review, at least annually, of all cryptographic standards and algorithms currently in use for critical systems, external linked or transactional customer-facing applications to prevent exploitation of weakened algorithms or protocols;
(d) the expansion of IT asset inventory to include all cryptographic tools and algorithms in use with pertinent information on the rationale for each cryptographic method employed and its mapping to supported application systems; and
(e) the development and testing of compromise-recovery plans in the event of a cryptographic key compromise. This must set out the escalation process, procedures for keys regeneration, interim measures, changes to business-as-usual protocols and containment strategies or options to minimise the impact of a compromise.

[21] Such as quantum computing.

S 10.21 A financial institution must conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non-repudiation of information. Additionally, a financial institution must ensure the following:

(a) except for non-critical systems or applications that do not contain customer information, the financial institution must retain ownership and control of the encryption keys (themselves or with an independent key custodian) to minimize the risk of unauthorised access to the data;

(b) where the financial institution does not generate its own encryption keys, the financial institution shall undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys securely including adhere to relevant industry standard;

(c) where this involves a reliance on third party assessments[22], the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance; and

(d) the financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.

S 10.22 A financial institution must ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. The protocols shall include secret and public cryptographic key protocols, both of which shall reflect a high degree of protection to the applicable secret or private cryptographic keys. The selection of such protocols must be based on recognised international standards and tested accordingly. Commensurate with the level of risk, secret cryptographic key and private-cryptographic key storage and encryption / decryption computation must be undertaken in a protected environment, supported by a hardware security module (HSM), trusted execution environment (TEE) or similarly secured devices.

S 10.23 A financial institution shall store public cryptographic keys in a certificate issued by a Certificate Authority, as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognised Certificate Authorities. The financial institution must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates must be consistent with industry best practices and applicable legal / regulatory specifications.

[22] For example, where the financial institution is not able to perform its own validation on embedded cryptographic controls due to the proprietary nature of the software or confidentiality constraints.

Data Centre Resilience

S 10.24 A financial institution must specify the resilience and availability objectives of its data centres to effectively support its business recovery objectives.

S 10.25 A financial institution must ensure data centres have redundant capacity components and multiple distribution paths serving the computer equipment to eliminate any single point of failure for effective achievement of the identified business recovery objectives.

S 10.26 A financial institution shall host critical systems in a dedicated space intended for production data centre usage. The dedicated space must be physically secured from unauthorised access and is not located in a disaster-prone area. A financial institution must also ensure there is no single point of failure in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure. A financial institution must also ensure adequate maintenance, and holistic and continuous monitoring of these critical components with timely alerts on faults and indicators of potential issues.

S 10.27 A financial institution must establish adequate control procedures for its data centre operations, including the deployment of relevant automated tools for batch processing management to ensure timely and accurate batch processes. These control procedures shall also include procedures for implementing changes in the production system, error handling as well as management of other exceptional conditions.

S 10.28 A financial institution must segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity[23]. In the case where vendors' or programmers' access to the production environment is necessary, these activities must be properly authorised and monitored.

Service Availability

S 10.29 A financial institution must ensure its system capacity needs are well-planned and managed with due regard to peak processing period, business growth plans and technology architecture changes.

S 10.30 A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services[24]. These monitoring mechanisms shall be capable of providing actionable alerts to administrators to enable timely detection and resolution of service interruptions. The monitoring scope, metrics and thresholds shall be updated periodically to ensure they remain effective.

[23] For example, system development activities must be segregated from data centre operations.
[24] For example, batch runs and backup processes for the financial institution's application systems and infrastructure.

S 10.31 A financial institution shall enhance the resilience of key digital services[25] and delivery channels[26] through the following measures:

(a) implement effective mechanisms by 30 September 2027 to provide early signals or warning of service degradation or intermittent failures. This means the capability to:

(i) detect failed transactions and measure service availability[27] more accurately;

(ii) monitor the number of affected customers and transaction volumes during service disruptions to measure the extent and severity customer impact; and

(iii) immediately escalating to senior management when service disruptions affect 5% or more of expected daily customers or transaction volumes;

(b) conduct regular reviews to identify and mitigate potentially vulnerable IT system interdependencies to prevent simultaneous interruptions to multiple digital services or delivery channels; and

(c) establish stand-in processing arrangement by 30 September 2027 and deploy such arrangement during disruptions to ensure continuity of services during disruptions. A financial institution shall prioritise deployment of this capability for digital services and delivery channels which are least substitutable[28], and ensure its customers are well informed on the terms of use (such as the transaction limit), associated risks and allocation of responsibilities between parties and mitigation actions against fraud risks.

S 10.32 For critical systems, where there is a reasonable expectation for immediate delivery of service to customers or dealings with counterparties, a financial institution must ensure that these systems are designed for high availability with a cumulative unplanned downtime affecting the interface with customers or counterparties of not more than 4 hours on a rolling 12 months basis and a maximum tolerable downtime of 120 minutes per incident.

G 10.33 Eligible e-money issuers, non-bank registered merchant acquirers and intermediary remittance institutions that have not been designated as a National Critical Information Infrastructure (NCII) entity are encouraged to implement the measures provided in paragraph 10.31.

S 10.34 A financial institution shall prioritise diversity[29] in technology to enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.

[25] Key digital services include balance enquiry for deposit accounts, domestic interbank fund transfers, DuitNow, FPX, RENTAS, bill payments and overseas fund transfers.

[26] Key delivery channels include internet banking, mobile banking, debit card or ATM (where relevant).

[27] For example, financial institutions should be able to distinguish between failed transactions caused by technical problems and scenarios involving customer inactivity or customer decision to abort.

[28] For example, customers may be unable to use ATM for large-value funds transfers when internet banking is disrupted or easily switch from a debit card to online banking channel for cashless parking payments or closed loop toll payments.

[29] Diversity in technology may include the use of different technology architecture designs and applications, technology platforms and network infrastructure.

S 10.35 During an interruption of digital services or delivery channels, including periods of performance degradation or intermittent failures, a financial institution shall respond promptly and effectively to minimise the impact on its customers. This includes but not limited to-

(a) ensure timely escalation and decision-making to resume services promptly via alternative arrangements and stabilise performance within the timeframe specified in paragraph 10.32 under all plausible scenarios;

(b) define clear accountabilities for managing performance degradation issues and formalise arrangements with third party service providers to ensure effective coordination and timely recovery to normal performance levels;

(c) establish a communication plan for service interruptions to immediately inform affected customers, properly manage a high volume of customer feedback, and provide frequent updates on recovery efforts, as well as actionable information on available alternatives for customers with urgent needs;

(d) provide customers with a convenient means of checking the availability of digital services, which may include publishing real-time availability and performance status of its digital services on the corporate website; and

(e) disclose the track record of service availability on a quarterly basis within 15 calendar days of quarter-end, beginning from 15 October 2027.

Network Resilience

S 10.36 A financial institution must design and implement a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans.

S 10.37 A financial institution must ensure the network services for its critical systems are reliable and have no single point of failure in order to protect the critical systems against potential network faults and cyber threats.

G 10.38 The control measures to prevent from network faults as referred to in paragraph 10.37 are expected to include component redundancy, service diversity and alternate network paths.

S 10.39 A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.

S 10.40 A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.

S 10.41 A financial institution must establish and maintain a network design blueprint identifying all of its internal and external network interfaces and connectivity. The blueprint must highlight both physical and logical connectivity between network components and network segmentations.

S 10.42 A financial institution must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years.

S 10.43 A financial institution must implement appropriate safeguards to minimise the risk of a system compromise in one entity affecting other entities within the group. Safeguards implemented may include establishing logical network segmentation for the financial institution from other entities within the group.

System backup and restoration

S 10.44 A financial institution must establish a robust backup strategy and procedures to meet business recovery objectives. At a minimum, a financial institution shall-

(a) establish backup and restoration procedures to effectively manage the backup data life cycle;
(b) maintain an adequate number of backup copies of all critical data, the updated version of the operating system software, production programs, system utilities, all master and transaction files and event logs for recovery purposes;
(c) backup media must be stored in an environmentally secure and access-controlled backup site;
(d) secure the storage and transportation of sensitive data in removable media to meet minimum controls as specified in **Appendix 1** or equivalent;
(e) test backup and restoration procedures periodically to validate recovery capabilities. Remedial actions shall be taken promptly by the financial institution to fix the root cause of unsuccessful backups; and
(f) undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times.

S 10.45 A financial institution shall establish a tamper-proof backup arrangement and an isolated recovery environment to enable timely resumption of critical banking and payment services within its tolerable level in the event of destructive cyber-attacks such as widespread data loss caused by ransomware.

Third Party Service Provider Management

S 10.46 The board and senior management of the financial institution must exercise effective oversight and address associated risks when engaging third party service providers[30] for critical technology functions and systems. The financial institution remains accountable for managing all risks that arise from engagement of third party service providers, to ensure security and reliability of technology services in compliance with all relevant regulatory requirements prescribed in this policy document.

S 10.47 A financial institution must conduct a due diligence on a third party service provider prior its on-boarding or engagement and throughout the service

[30] The financial institution must adhere to the requirements in the policy document on Outsourcing for engagements with third party service providers that meet the definition of outsourcing arrangement as specified in the policy document.

engagement to ensure achievement of business performance and recovery objectives remain unimpaired, considering the latest risk environment. At the minimum, a financial institution must consider the range of risks outlined in **Appendix 8**.

S 10.48 A financial institution must establish a Service Level Agreement (SLA) when engaging third party service provider. At a minimum, the SLA shall contain the following:

(a) access rights for the regulator and any party appointed by the financial institution to examine any activity or entity of the financial institution. This shall include access to any record, file or data of the financial institution, including management information and the minutes of all consultative and decision-making processes;

(b) requirements for the third party service provider to provide sufficient prior notice to financial institutions of any sub-contracting which is substantial;

(c) a written undertaking by the third party service provider on its compliance with secrecy provisions under relevant legislations. The SLA shall further clearly provide for the third party service provider to be bound by integrity and confidentiality provisions stipulated under the contract even after the engagement has ended;

(d) arrangements for disaster recovery and backup capability, where applicable;

(e) service level objectives for uptime or availability;

(f) arrangements to secure business continuity in the event of an exit or termination of the third party service provider, which includes ensuring data residing in third party service providers are recoverable in a timely manner;

(g) responsibility of third party service providers to promptly disclose and notify the financial institution[31] of any service disruptions or cyber incidents that affect the financial institution or its customer data that occur within such service providers' or sub-contractors' environment.

(h) requirements for the third party service providers to comply with the relevant internationally recognised standards and ensure their key staff keep their skills up-to-date with the relevant certifications; and

(i) requirements for third party service providers to participate in the financial institution's security awareness and education program, where appropriate.

[31] This enables financial institutions to provide timely updates to the Bank and other relevant regulatory bodies, subject to the applicable secrecy provisions under relevant legislations.

S 10.49 A financial institution must formulate a roadmap to achieve continuous monitoring of a third party service provider's cybersecurity posture to obtain real-time insights for effective incident management. The financial institution shall undertake the following:

(a) measure the IT infrastructure footprint and the customer information accessible to third parties, and regularly manage this external stress state exposures to mitigate cyber-attack surfaces;
(b) adopt leading security policies and controls to mitigate product-specific third party risks;
(c) ensure incident response plans incorporate protocols with third party service providers to detect and contain adverse impact of security vulnerabilities resulting from software updates;
(d) define a priority set of security controls that require more frequent assurance assertion from the third party service providers;
(e) monitor technology and cyber incidents information disclosed by third party service providers at a higher frequency;
(f) implement technology solutions to automate metric testing; and
(g) establish processes to respond to breached thresholds, including investigating failed assertions and remedying control gaps.

Cloud Services

S 10.50 A financial institution must fully understand the inherent risk of adopting cloud services. In this regard, a financial institution shall conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet. The assessment must specifically address risks associated with the following:

(a) sophistication of the deployment model;
(b) migration of existing systems to cloud infrastructure;
(c) location of cloud infrastructure including potential geo-political risks and legal risks that may impede compliance with any legal or regulatory requirements;
(d) multi-tenancy or data co-mingling;
(e) vendor lock-in and application portability or interoperability;
(f) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection;
(g) exposure to cyber-attacks via cloud service providers;
(h) termination of a cloud service provider including the ability to secure the financial institution's data following the termination;
(i) demarcation of responsibilities, limitations and liability of the cloud service provider; and
(j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.

G 10.51 For critical systems hosted on a public cloud[32], a financial institution is expected to consider common key risks and control measures as specified in **Appendix 10**. A financial institution that relies on alternative risk management practices that depart from the measures outlined in **Appendix 10** is expected to be prepared to explain and demonstrate to the Bank that

[32] Refer the Special Publication 800-145 on Definition of Cloud Computing issued by the National Institute of Standards and Technology, U.S. Department of Commerce.

these alternative practices are at least as effective as, or superior to, the measures in **Appendix 10**.

S 10.52 A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.

Access Control

S 10.53 A financial institution must implement an access control policy for the identification, authentication, and authorisation of all users to its IT assets and data. The level of granularity defined in the access control policy shall be commensurate with the level of risk of unauthorised access to its IT assets.

S 10.54 A financial institution shall adhere to the following principles:

(a) adopt a "deny all" access control policy for users by default because all access to IT assets must be explicitly authorised;
(b) employ "least privilege" access rights to ensure IT assets are accessed on a "need-to-have" basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;
(c) employ time-bound access which restrict access to a specific period based on the nature of work;
(d) employ segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features. This may include a combination of functions such as:
    (i) system development and technology operations;
    (ii) security administration and system administration;
    (iii) network operation and network security; and
    (iv) IT operations environment;
(e) establish criteria for activities that require dual authorization control; and
(f) adopt robust user authorization and authentication based on criticality of IT assets as follows:
    (i) stronger authentication for critical activities and higher-risk environment such as remote access;
    (ii) ensure user credentials provisioned with robust identity verification method to prevent impersonation risks; and
    (iii) ensure online credential is uniquely linked to a single user to ensure clear accountability in access to confidential IT assets.

S 10.55 A financial institution must employ a multi-factor authentication (MFA) that can defend against social engineering attacks for authenticating user access to critical systems. The MFA must combine two or more of knowledge factors, inherent factors (e.g. biometric characteristics) or possession factors (e.g. security keys, tokens).

S 10.56 A financial institution must establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix must be periodically reviewed and updated.

S 10.57 A financial institution must ensure-

(a) access controls to enterprise-wide systems are effectively managed and monitored;

(b) anomalies are flagged for prompt investigations to contain any cyber incidents; and

(c) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.

The rest of the page is intentionally left as blank

11 Cybersecurity Management

Cyber Risk Management

S 11.1 A financial institution must ensure that there is an enterprise-wide focus on effective cyber risk management to reflect the collective responsibility of business and technology lines for managing cyber risks.

S 11.2 A financial institution must develop a CRF which clearly articulates its governance for managing cyber risks, its cyber resilience objectives and its risk tolerance, with due regard to the evolving cyber threat environment. Objectives of the CRF shall include ensuring operational resilience against extreme but plausible cyber-attacks. The framework must be able to support the effective identification, protection, detection, response, and recovery (IPDRR) of systems and data hosted on-premises or by third party service providers from internal and external cyber-attacks.

S 11.3 The CRF must consist of, at a minimum, the following elements:

(a) development of an institutional understanding of the overall cyber risk context in relation to the financial institution's business and operations, its exposure to cyber risks and current cybersecurity posture;

(b) identification, classification and prioritisation of critical systems, information, assets and interconnectivity (with internal and external parties) to obtain a complete and accurate view of the financial institution's information assets, critical systems, interdependencies and cyber risk profile;

(c) identification of cybersecurity threats, vulnerabilities and countermeasures to secure digital services delivery against cyber-attacks and contain reputational damage that can undermine confidence in the financial institution;

(d) enhancing layers of cyber defence with reference to the latest international standards and sound practices such as zero-trust principles[33], defense-in-depth through micro-segmentation and security by design, to protect its data, infrastructure and assets against evolving cyber threats;

(e) timely detection of cybersecurity incidents through continuous surveillance and monitoring;

(f) detailed incident handling policies and procedures and a crisis response management playbook to support the swift recovery from cyber incidents and contain any damage resulting from a cybersecurity breach;

(g) policies and procedures for timely and secure information sharing and collaboration with other financial institutions and participants in financial market infrastructure to strengthen cyber resilience and fraud prevention;

(h) implement a centralised automated tracking system to manage its technology asset inventory; and

(i) establish a cyber risk management function to analyse actual and potential cyber threats, providing risk assessments and timely

[33] Zero-trust principles is a security paradigm designed to prevent data breaches and limit lateral movement of threat actors by requiring all users, whether in or outside the organization's network, to be authenticated, authorised, and validated before being granted the access.

escalation of high-risk cyber threats to senior management and the board. This function shall be performed by an in-house dedicated team or by leveraging on the parent or group.

S 11.4 A financial institution that is designated as a National Critical Information Infrastructure (NCII) entity pursuant to the Cyber Security Act 2024 must ensure compliance to the requirements and guidelines applicable to NCII, including any additional directives and standards issued by the National Cyber Security Agency (NACSA).

S 11.5 A financial institution must adopt robust control measures as outlined in **Appendix 5** to enhance its resilience to cyber-attacks.

S 11.6 A financial institution must conduct a realistic "Red Team[34]" simulation attack on its infrastructure at least once every three years to proactively identify and manage potential vulnerabilities.

G 11.7 A financial institution may implement crowdsourced security testing programs as a complement to existing security assessments, in order to thoroughly test the security of their IT environment. The financial institution must engage reputable and credible service providers to facilitate the program.

Cybersecurity Operations

S 11.8 A financial institution must establish clear responsibilities for cybersecurity operations which shall include implementing appropriate mitigating measures in the financial institution's conduct of business that correspond to the following phases of the cyber-attack lifecycle:

(a) reconnaissance;
(b) weaponisation;
(c) delivery;
(d) exploitation;
(e) installation;
(f) command and control; and
(g) exfiltration.

S 11.9 A financial institution must ensure continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure to prevent potential compromise of its security controls or weakening of its security posture. This shall include-

(a) establishing a Security Operations Center (SOC) supported by competent resources and equipped with the necessary tools and technologies for proactive monitoring of its technology security posture;

[34] A red team exercise involves a controlled attempt to rigorously evaluate an institution's security defences, resilience, and response capabilities. In this exercise, a team of information security experts known as the "red team" simulates the tactics, techniques, and procedures of potential adversaries to critically assess the effectiveness of the institution's security measures, with minimal knowledge and impact on operations.

(b) ensuring the scope of monitoring must cover all critical systems including the supporting infrastructure; and

(c) conducting regular review of its security posture via the conduct of a vulnerability assessment and penetration testing in line with **Appendix 5**.

S 11.10 A financial institution must establish a process to collect, analyse and evaluate cyber threat information in relation to its environment ("cyber threat intelligence") to promptly detect cyber threats, including data breach incidents and spread of misleading information in relation to the financial institution over the Internet[35].

S 11.11 A financial institution must establish appropriate response to investigate and respond to flagged anomalous activities based on their level of complexity.

Cyber Response and Recovery

S 11.12 A financial institution must establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the organisation's overall crisis management plan, escalation processes, business continuity and disaster recovery planning. This includes developing a clear communication plan for engaging shareholders, regulatory authorities, customers and employees in the event of a cyber incident.

S 11.13 A financial institution must establish and implement a comprehensive Cyber Incident Response Plan (CIRP). The CIRP must address the following:

(a) **Preparedness**
Establish a clear governance process, reporting structure and roles and responsibilities of the Cyber Emergency Response Team (CERT) as well as invocation and escalation procedures in the event of an incident;

(b) **Detection and analysis**
Ensure effective and expedient processes for identifying points of compromise, assessing[36] the extent of damage and preserving sufficient evidence for forensics purposes;

(c) **Containment and eradication**
Identify and implement remedial actions to prevent or minimise damage to the financial institution, contain and remove the known threats and resume business activities;

(d) **Recovery**
Implement multiple strategies including contingency plans as part of incident recovery to swiftly resume business operations and significantly enhance redundancy and resilience; and

[35] This includes the capability to collect and correlate such information from sources such as social media and dark web.
[36] This includes competency in handling threat actor claims by confirming the legitimacy and extent of the incident and uncover more details on the threat actor.

(e) **Post-incident activity**
Conduct post-incident review incorporating lessons learned and develop long-term risk mitigations.

S 11.14 A financial institution must ensure that relevant CERT members are conversant with the incident response plan and handling procedures and remain contactable at all times.

S 11.15 A financial institution shall establish a secure and reliable out-of-band communication infrastructure for both internal and external stakeholders to ensure continued coordination and communication if the primary communication infrastructure is compromised or rendered unavailable during a crisis.

S 11.16 A financial institution must conduct an annual cyber drill exercise to test the effectiveness of its CIRP including the out-of-band communication methods, based on various current and emerging threat scenarios (e.g. social engineering), with the involvement of key stakeholders including members of the board, senior management and relevant third party service providers. The result of the annual cyber drill exercise must be reported to the board in a timely manner. The out-of-band communication methods must also be tested regularly as part of the institutions cyber drill exercises. The test scenarios must include scenarios designed to test-

(a) the effectiveness of escalation, internal and external communication and decision-making processes that correspond to different impact levels of a cyber incident; and
(b) the readiness and effectiveness of CERT and relevant third party service providers in supporting the recovery process.

S 11.17 A financial institution shall review its loss provision arrangements to ensure its adequacy to cover cyber incidents based on its scenario analysis of extreme adverse events. Where cyber insurance is adopted to mitigate impact of cyber incidents, the financial institution shall-

(a) ensure that the scope of the insurance policy adequately covers the information security events and types of liability that the financial institution is exposed to;
(b) understand the terms and conditions of the insurance policy in relation to warranties, attestations or any responsibilities of the financial institution, have them reflected in the crisis response policies and procedures as appropriate and ensure that any changes to IT services and control measures do not result in unintended exclusions of cover; and
(c) ensure that any obligations imposed by the insurance policy (such as in relation to appointment of experts and accepting their recommendations during a cyber incident) do not impair its ability to act in the best interest of the financial institution and its customers. The financial institution shall anticipate and adequately manage any conflict of interest that may arise from the objective of the insurer to minimise the cost of its liability under the insurance policy.

Cyber Reporting and Threat Information Sharing

S 11.18 A financial institution is required to notify the Bank of cyber incidents in adherence to the Bank's policy documents on Operational Risk Reporting – Part C, Business Continuity Management – Part C, Merchant Acquiring Services – paragraphs 19.25 to 19.26 and any other relevant policy documents specified by the Bank.

S 11.19 Subject to the applicable data protection laws, a financial institution must share cyber threat intelligence information with the industry on a timely basis via the relevant sharing platforms developed by the Bank, the industry, or law enforcement agencies. In addition, the financial institution must allocate resources to participate in any industry-wide initiatives aimed at improving collective threat intelligence capabilities.

S 11.20 A financial institution shall collaborate and cooperate closely with relevant stakeholders and authorities in combating cyber threats.

The rest of the page is intentionally left as blank

12 Digital Services

Security of Digital Services

S 12.1 Securing digital services is an integral part of financial institution's risk management. A financial institution must expand its CRF to implement robust technology security controls in providing digital services which assure the following:

(a) adopt and regularly assess the minimum-security controls for respective delivery channels to ensure confidentiality and integrity of customer and counterparty information and transactions. Refer to **Appendices 2, 3, 4** and **11**;

(b) proper authentication of users or devices and authorization of transactions to mitigate impersonation and fraud risk. Refer the minimum-security controls in **Appendix 3**; and

(c) strong physical control and logical control measures.

S 12.2 In the event that a financial institution has not yet implemented the digital services security controls specified under paragraph 12.1 to 12.9, the financial institution must-

(a) be ready to provide documented explanation of how alternatives measures or mitigations achieve equivalent or superior effectiveness; and

(b) assume the liability of any fraud that occurs due to the gaps arise from the absence of the specified control.

Digital Fraud Management and Customer Awareness

S 12.3 The complex and fast evolving digital fraud requires financial institutions to be vigilant against new fraud techniques and proactive in strengthening their cyber defence for customer protection. In line with paragraphs 11.2 and 11.3, a financial institution must enhance its CRF as follows:

(a) expand the scope of identification of cybersecurity threats and countermeasures to include customers' mobile devices and access points;

(b) adopt layered (defense-in-depth) security controls to protect the digital service application deployed to customers' mobile devices and the relevant banking data contained in it;

(c) perform continuous surveillance and monitoring to detect any exploitation of the digital service application deployed to customers' mobile devices and ensure the swift upgrade of security controls to mitigate new vulnerabilities;

(d) establish clearly defined and effective incident handling procedures to assist customers to contain the potential damage resulting from a cybersecurity breach involving digital services;

(e) formalise operational arrangement to enable swift coordinated response and rapid upgrade of countermeasures to defend against advanced fraud tactics if a financial institution relies on multiple business functions;

(f) conduct regular review by senior management to ensure the effectiveness of digital fraud management and define threshold for escalation of countermeasures considering the actual impact to victims of digital fraud and emerging fraud environment; and

(g) apprise the board on the outcome of management reviews to preserve public confidence in the security of digital services and mitigate reputation risk to the industry.

S 12.4 A financial institution must ensure that its fraud detection capabilities and rules are updated in a timely manner upon detection of new fraud modus operandi in order to prevent fraudulent transactions or account takeover using stolen customer credentials. This must be supported by appropriate risk analytics to improve the accuracy of fraud detection, that includes continuous upgrade of fraud detection capabilities as specified in **Appendix 11** on Fraud Detection Standards.

S 12.5 A financial institution must mitigate any attendant risk arising from its delivery of digital services. This shall include-

(a) adopt secure communication channel to mitigate risk of phishing. Compensating controls shall be adopted when using communication channel prone to phishing exploits[37];
(b) all customers must be properly informed in advance of new controls to ease adoption and minimise inconvenience; and
(c) practical ways for customers to verify the authenticity of calls made by the financial institution or its appointed outsourced service providers.

S 12.6 A financial institution shall empower customers to mitigate digital fraud risks where it is reasonably practical. This shall include offering customer mechanisms to manage activation and de-activation of payment card[38] for card-not-present and overseas transactions. This shall not absolve the financial institution from its liabilities, responsibilities and duty of care to ensure the security of its digital services.

S 12.7 Consumer competency is essential to strengthening the security of digital services. A financial institution must maintain continuous efforts to review and enhance the effectiveness of its awareness programmes, ensuring customers understand the risks of digital services fraud. This shall include-

(a) continuous and timely updates of practical information on how to identify potential fraud, including specific information about new or common modus operandi;
(b) clear explanation about new and existing security measures, such as how to verify genuine e-banking websites and mobile applications;
(c) real-time alerts of possible risks when security measures are absent or have not yet been implemented; and
(d) measures to further improve customer understanding and familiarisation with fraud risks and controls, such as through interactive simulations of security features etc.

S 12.8 A financial institution must provide convenient means for customers to report, suspend and re-activate their account swiftly in the event of a suspected fraud, where applicable. This shall require the financial institution to:

[37] A financial institution must remove any clickable hyperlinks in short messaging service (SMS) messages to customers and create awareness on this change to mitigate risk of phishing.
[38] A financial institution must adhere to the relevant requirements of the policy documents, as issued by the Bank, on Debit Card and Debit Card-I, and Credit Card and Credit Card-I in managing opt-in requirement for card-not-present and overseas transactions.

(a) offer a secure self-service “kill switch” solution;
(b) ensure that its contact centre is adequately resourced and operating effectively to provide prompt and adequate assistance to customers in distress; and
(c) restore customer access to digital services within a reasonable timeframe upon validation.

S 12.9 In addition to effective incident handling procedures, a financial institution must adopt additional measures to mitigate risk to customers arising from any incident involving potential fraud or compromise of customer data. This shall include-

(a) heighten monitoring of affected customer accounts;
(b) notify affected customers and provide them with the necessary information to apply mitigating measures and reduce the risk of fraud; and
(c) revoke and re-issue affected user credentials or designated payment instruments, where there is a potential risk of exploitation due to compromised data or other fraudulent activity.

The rest of the page is intentionally left as blank

13 Technology Audits

Audit function

S 13.1 A financial institution must ensure that the scope, frequency, and intensity of technology audits are commensurate with the complexity, sophistication and criticality of technology systems and applications.

S 13.2 A financial institution must establish annual review on its technology audit plan that provides appropriate frequency and coverage of critical technology services, third party service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post-implementation review of new or material enhancements of technology services.

S 13.3 A financial institution must ensure the internal audit function must have dedicated technology audit resources with specialised competencies and professionally certified. The technology audit resources shall be adequately conversant with the developing sophisticate of the financial institution's technology systems, delivery channels and have sound knowledge in the areas audited.

G 13.4 The technology audit resources may be enlisted to provide advice on compliance and adequacy of control processes during the planning and development phases of new major products, systems, adoption of third party service providers or technology operations. In such cases, the technology auditors participating in this capacity are expected to carefully consider whether such an advisory or consulting role can materially impair their independence or objectivity in performing post-implementation reviews of the products, systems and operations concerned.

14 External Party Assurance

S 14.1 A financial institution shall appoint a technically competent external service provider to carry out a production data centre resilience and risk assessment (DCRA). The assessment must consider all major risks and determine the current level of resilience of the production data centre. A financial institution must ensure the assessment is conducted at least once every three years or when there is a material change in the data centre infrastructure, whichever is earlier. The assessment shall, at a minimum, include a consideration of whether the requirements in paragraphs 10.24 to 10.28 have been adhered to. For data centres managed by third party service providers, a financial institution shall only rely on independent third party assurance reports provided such reliance is consistent with the financial institution's risk appetite and tolerance, and the independent assurance has considered similar risks and meets the requirements in this paragraph for conducting the DCRA. The designated board-level committee specified in paragraph 8.3 must deliberate the outcome of the assessment.

S 14.2 A financial institution shall appoint a technically competent external service provider to carry out regular network resilience and risk assessments (NRA) and set proportionate controls aligned with its risk appetite. The assessment must be conducted at least once in three years or whenever there is a material change in the network design, whichever is earlier. The assessment must consider all major risks and determine the current level of resilience. This shall include an assessment of the financial institution's adherence to the requirements in paragraphs 10.36 to 10.43. The designated board-level committee specified in paragraph 8.3 must deliberate the outcome of the assessment.

15 Security Awareness and Education

S 15.1 A financial institution must provide adequate and regular technology and cybersecurity awareness education for all staff in undertaking their respective roles and measure the effectiveness of its education and awareness programs. This cybersecurity awareness education must be conducted at least annually and must reflect the evolving cyber threat landscape and emerging risks. Where appropriate, the financial institution shall also include its third party service providers in their relevant training as outlined in paragraph 10.48(i).

S 15.2 A financial institution must provide adequate and continuous training for staff involved in technology operations, cybersecurity and risk management in order to ensure that the staff are competent and suitably certified to effectively perform their roles and responsibilities.

S 15.3 A financial institution must provide its board members with regular training and information on technology developments to enable the board to effectively discharge its oversight role.

PART C REGULATORY PROCESS

16 Notification for Technology-Related Applications

Introduction or enhancement to digital services

S 16.1 A financial institution must notify the Bank in accordance with the requirements in paragraphs 16.2 to 16.7 prior to introducing new digital services or enhancement to existing digital services.

S 16.2 A financial institution offering digital services for the first time must undertake measures specified under paragraph 16.4 and submit the following information in the notification to the Bank:

(a) assessment on the risks identified and strategies to manage such risks. This includes specific accountabilities, policies and controls to address risks;
(b) security arrangements and controls;
(c) significant terms and conditions;
(d) client charter;
(e) privacy policy statement; and
(f) any outsourcing or website link arrangements, or strategic alliances or partnerships with third parties that have been finalised.

S 16.3 For any enhancements to existing digital services which meet the criteria in **Appendix 6**, a financial institution shall be subject to a simplified notification requirement and submit the following information in the notification to the Bank:

(a) description of the enhancements to the existing technologies; and
(b) risk assessment of the proposed enhancements, including the impact and measures to mitigate identified risks.

S 16.4 For any enhancements to existing digital services which are not subject to the simplified notification requirement under paragraph 16.3, a financial institution is required to undertake the following measures prior to notifying the Bank:

(a) engage an independent external party to provide assurance that the financial institution has addressed the technology risks and security controls associated with the digital services or any material enhancement to the digital services. The format of the assurance shall be as set out in **Part A of Appendix 7**; and
(b) provide a confirmation by the CISO, senior management officer or the chairman of the board or designated board-level committee specified in paragraph 8.3 of the financial institution's readiness to provide digital services or implement any material enhancement to the digital services. The format of the confirmation shall be as set out in **Part B of Appendix 7.**

S 16.5 A financial institution must ensure that the independent external party providing the assurance is competent and has a good track record. The assurance shall address the matters covered in, and comply with, **Part C and D of Appendix 7.**

S 16.6 A financial institution shall provide relevant documents for the Bank's review when required by the Bank.

G 16.7 A financial institution may offer digital services or implement any enhancement to the digital services immediately upon submission of the notification under paragraph 16.1 and compliance with the requirements in paragraphs 16.2 to 16.6.

17 Consultation and Notification related to Cloud Services and Emerging Technology

S 17.1 A financial institution is required to consult the Bank prior to the first-time adoption of a public cloud or emerging technology for critical systems. During the consultation, the financial institution must demonstrate that specific risks associated with the use of these technologies have been adequately considered and addressed to the satisfaction of the Bank, in order to proceed with the adoption of the public cloud for critical systems for the first time. The financial institution shall undertake the following prior to consulting the Bank on its adoption of public cloud for critical systems:

(a) conduct a comprehensive risk assessment of the proposed cloud adoption or emerging technology, including the possible impact and measures to address and mitigate the identified risks. For public cloud, the assessment must follow the risk outlined in paragraph 10.50 and **Appendix 10**. For emerging technology, it must follow the guideline in **Appendix 9**. The financial institution shall also adopt the format of the Risk Assessment Report as per **Part A of Appendix 7**;

(b) provide a confirmation by the CISO, senior management officer or the chairman of the board or designated board-level committee specified in paragraph 8.3 of the financial institution's readiness to adopt public cloud or emerging technology for critical system. The format of the confirmation shall be as set out in **Part B of Appendix 7**; and

(c) perform a third party pre-implementation review on public cloud or emerging technology. This review shall encompass the areas set out in **Appendix 10** (for public cloud) or **Appendix 9** (for emerging technology) and **Part C of Appendix 7** for higher-risk services, such as those involving the processing or storage of customer information, or cross-border data transmission.

S 17.2 A financial institution shall notify the Bank on any subsequent adoption of a public cloud or emerging technology for critical system, by submitting the notification together with the necessary updates to all the information required under paragraph 17.1, subject to the financial institution having complied with the following requirements and included documentation and information to demonstrate such compliance in the notification submitted to the Bank that the financial institution:

(a) has consulted the Bank prior to adopting a public cloud or emerging technology for critical systems for the first time in accordance with paragraph 17.1, with no concerns raised by the Bank during the first-time consultation;

(b) has enhanced the technology risk management framework to manage cloud or emerging technology risks;
(c) has established independent assurance on the cloud risk management framework or emerging technology risk management framework; and
(d) has provided assurance to the Bank that the incident response plans are sufficient to cater for adverse or unexpected events.

G 17.3 For the avoidance of doubt, notification to the Bank under paragraph 17.2 is not required for any enhancement to existing cloud adoption and emerging technology adoption that does not materially alter the prior assessments and representations made by a financial institution to the Bank.

S 17.4 The Bank may at its discretion direct a financial institution to consult the Bank under paragraph 17.1, notify the Bank under paragraph 17.2 or observe any of the guidance in **Appendix 10** or **Appendix 9** and to explain any deviations from the guidance in **Appendix 10** or **Appendix 9**, including for a non-critical system or when the pre-requisites in the paragraphs 17.1 or 17.2 have not been met. A financial institution must comply with such a directive promptly and to the satisfaction of the Bank.

S 17.5 A financial institution must ensure the roadmap for adoption of cloud services or emerging technology (for critical systems and non-critical systems) is included in the annual outsourcing plan submitted to the Bank in adherence with the requirements in the policy document on Outsourcing or IT Profile reporting. The risk assessment as outlined in paragraph 10.50 for cloud services or **Appendix 9** for emerging technology must also be documented and made available for the Bank's review as and when requested by the Bank.

18 Assessment and Gap Analysis

S 18.1 A financial institution must perform a gap analysis of existing practices in managing technology risk against the requirements in this policy document and highlight key implementation gaps. The financial institution must develop an action plan with a clear timeline and key milestones to address the gaps identified. The gap analysis and action plan must be submitted to the Bank no later than 90 days after the issuance date of this policy document. Financial institutions that have previously made a submission in accordance with the equivalent provision in the previous version of this policy document are required to maintain continuous compliance by identifying any new gaps against the enhanced or revised requirements in the latest version of this policy document and taking the necessary steps to address such gaps. The updated annual assessment of its level of compliance must be made available to the Bank upon request.

S 18.2 The self-assessment, gap analysis and action plan in paragraph 18.1 must be submitted to Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan, Jabatan Penyeliaan Insurans dan Takaful or Jabatan Pemantauan Perkhidmatan Pembayaran, as the case may be.

Appendix 1 Storage and Transportation of Sensitive Data in Removable Media

Financial institutions must ensure adequate controls and measures are implemented for the storage and transportation of sensitive data in removable media, including:

1. deploying the latest industry-tested and accepted encryption techniques;
2. implementing authorised access control to sensitive data (e.g. password protection, user access matrix);
3. prohibiting unauthorised copying and reading from the media;
4. where there is a need to transport the removable media to a different physical location, financial institutions must-
   (a) strengthen the chain of custody processes for media management which includes:
      (i) the media must not be under single custody at any point of time;
      (ii) the media must always be within sight of the designated custodians; and
      (iii) the media must be delivered to its target destination without unscheduled stops or detours;
   (b) use secure and official vehicle for transportation;
   (c) use strong and tamper-proof containers for storing the media with high-security lock (e.g. dual key and combination lock); and
   (d) implement location tracking functionality for each media container; and
5. ensuring third party service providers comply with the requirements in paragraphs 1 to 4 of this Appendix, in the event third party services are required in undertaking the storage management or transportation process of sensitive data.

Appendix 2 Control Measures on Self-service Terminals (SSTs)

Cash SST

Cash SSTs are computer terminals provided by banking institutions such as Automated Teller Machine, Cash Deposit Machine and Cash Recycler Machine that provide cash transactions such as cash withdrawals and deposits including in foreign currencies.

Financial institutions must ensure the adequacy of physical and logical security and controls implemented on the Cash SST, which includes-

1. enforcing full hard disk encryption;
2. retaining cards or block access to Cash SST service when the following are detected:
   (a) exceed maximum PIN attempts;
   (b) invalid card authentication value;
   (c) cash SST card unable to eject;
   (d) “deactivated” card status;
   (e) inactive account status such as “Dormant” or “Deceased”; and
   (f) cards tagged as “Lost” or “Stolen”;
3. deploying antivirus solution for Cash SST, ensure full virus scanning on all Cash SSTs is performed periodically and ensuring timely update of signatures;
4. implementing a centralised management system to monitor and alert any unauthorised activities on Cash SST such as unauthorised shutting-down of operating system or deactivation of the white-listing programme;
5. ensuring effective control over the Cash SST lock and key by using a unique and non-duplicable key to open the Cash SST PC Core compartment as well as ensure proper safekeeping and custody of the key;
6. installing alarm system with triggering mechanism connected to a centralised alert system to detect and alert bank’s staff of any unauthorised opening or tampering of the physical component of the Cash SST, particularly the access to the Cash SST PC Core;
7. securing physically the Cash SST PC Core by enclosing the central processing unit (CPU) in a locked case;
8. enforcing pairing authentication for key Cash SST components, particularly between cash dispenser and Cash SST controller;
9. enforcing Basic Input Output System (BIOS) lock-down which includes:
   (a) enabling unique password protection for accessing BIOS. The password shall be held by financial institutions under strict control;
   (b) disabling external input device and port such as CD-ROM, floppy disk and USB port. The Cash SST operating system can only be booted from the internal hard disk; and
   (c) disabling automatic BIOS update;
10. ensuring proper configuration and hardening of the operating system and application system, which includes:

(a) blocking any wireless network connection such as Bluetooth, Wi-Fi;
(b) disabling Microsoft default program system (such as Notepad, Internet browser, Windows shortcut, file download, file sharing and command prompt);
(c) disabling unnecessary services in the operating system such as the auto-play features;
(d) concealing Start Bar or Tray Menu;
(e) enabling cache auto-deletion; and
(f) disabling key combinations and right-click mouse functions;

11. enforcing secure system parameter setting, which includes-

(a) changing default passwords and other system security parameters setting of the Cash SST;
(b) using a unique system administrator password for all Cash SSTs; and
(c) using lowest-level privileges for programmes and users' system access;

12. enforcing and monitoring of Cash SST end-point protection such as installing white-listing programmes. The end-point protection programme, at a minimum, shall ensure only authorised Cash SST system processes and libraries are installed and executed;

13. enforcing strict control procedures over installation and maintenance of Cash SST operating systems and application systems, which includes-

(a) ensuring only authorised personnel have access to gold disk copy (master copy of Cash SST installation software);
(b) ensuring the gold disk copy is scanned for virus / malware prior to installation into Cash SST; and
(c) enforcing dual control for installation and maintenance of Cash SST software; and

14. installing closed-circuit cameras and transaction triggered cameras at strategic locations with adequate lighting in order to ensure high quality and clear closed-circuit television images of cardholder performing a transaction as well as any suspicious activities.

Non- Cash SST

Non-cash SSTs are computer terminals such as desktops, laptops, tablets, kiosks or machines that provide non-cash transactions such as cheque deposits, balance enquiries, fund transfers, card replacements, utilities bill payments or insurance quotations.

Financial institutions must ensure the adequacy of physical and logical security and controls implemented on the self-service terminals, which includes-

1. enforcing the use of lock and key on the computer terminal's CPU at all times;
2. deploying closed-circuit television to monitor the usage of self-service terminals;
3. disabling the use of all input devices (such as USB, CD and DVD), application system (such as Notepad, Microsoft Word, and Microsoft PowerPoint) and file download as well as command prompt on the kiosk;
4. disabling browser scripting, pop-ups, ActiveX, Windows shortcut;
5. concealing Start Bar or Tray Menu;
6. enabling cache auto-deletion;
7. disabling key combinations and right-click mouse functions; and
8. restricting use of Internet browser i.e. only to be used to access the financial institution's internet website.

Appendix 3 Control Measures for Digital Services

1. A financial institution must ensure the adequacy of security controls implemented for digital services, which include the following, where relevant:

   (a) ensure registration or enrolment of digital services is subject to robust authentication and verification;

   (b) ensure transactions are performed over secured channels such as the latest version of Transport Layer Security (TLS);

   (c) ensure that both client and host application systems encrypt all confidential information prior to transmission over the network;

   (d) implement strong mutual authentication between the users' end-point devices and financial institutions' servers, such as the use of the latest version of Extended Validation SSL certificate (EV SSL);

   (e) ensure secure user and session handling management;

   (f) ensure sufficient and relevant digital service logs are retained for investigations and forensic purposes for at least three years;

   (g) put in place additional authentication protocols to enable customers to identify the financial institution's genuine website such as deploying image or word verification authentication or similar controls. The system shall require the customer to acknowledge that the image or word is correct before the password box is displayed to the customer;

   (h) ensure resilience against brute-force attacks[39];

   (i) for new customers, the default transfer limit shall be set at a conservatively low level (such as RM1,000 per day). However, customers shall be provided with the option to change the limit via secure channels (e.g. online with multi-factor authentication (MFA) or at branches); and

   (j) apply appropriate verification and cooling-off period for first time enrolment of digital services or secure device, transaction limit increase or other activities which deemed necessary.

[39] A brute-force attack is a method used by attackers to gain unauthorised access to a system by systematically trying possible combinations or attempting to guess passwords or encryption keys.

2. A financial institution must ensure technology used in identity proofing and authentication methods are -
   (a) secure, highly resistant to cyber threats[40] affecting customer devices, including but not limited to malware, phishing, unauthorised access and data leakage;
   (b) accurate, have a minimal false acceptance rate to ensure confidentiality, integrity and non-repudiation of transactions across all authentication methods, including biometrics, tokenized processes, and contactless systems; and
   (c) compliant with internationally recognised standards where available and ensuring consistency and reliability in the security and performance of digital services.

3. A financial institution must strengthen security controls for registration and update of mobile device and customer details (such as mobile number, email and postal address) used for authentication of digital service transactions to prevent fraudsters from initiating funds transfers using stolen credentials. This shall include-
   (a) ensure secure binding and unbinding processes for restricting that authentication of digital service transactions by default to one mobile device or secure device per account holder (or to designated devices in the case of joint or business accounts), except when specifically requested by customers who understand and accept the risks of dispensing with this control;
   (b) ensure all customers are immediately alerted upon detecting access to the customer's account from a new device, or when customer details are changed;
   (c) ensure that the registration of new mobile phone number or replacement of existing mobile phone number is only processed after applying robust verification methods to confirm the authenticity of the customer;
   (d) adopt efficient measures to promptly verify and assist customers who need to change devices or update their personal details; and
   (e) apply appropriate verification and cooling-off period for first time enrolment of digital services or secure device and multiple successive high-volume transactions or other abnormal transaction patterns. Transaction limit increase must also be subject to appropriate verification.

4. A financial institution must implement controls to authenticate devices and users, authorise transactions, and support non-repudiation and accountability for transactions performed via digital services. These measures must include, at a minimum, the following:
   (a) adopt MFA for financial and high-risk non-financial transactions. This includes when registering an account as a "favourite" beneficiary and, for all subsequent funds transfer to the favourite beneficiary;
   (b) request users to verify details of the transaction prior to execution; and
   (c) provide timely notification to customers that is sufficiently descriptive of the nature of the transaction.

[40] This includes but not limited to malware, phishing, transaction fraud or data leakage.

5. A financial institution must ensure the MFA solution used to authenticate financial transactions are adequately secure and resistant to phishing attacks, which includes the following:
   (a) activation of MFA must be subject to robust verification by the financial institution;
   (b) timely notification to customers of any activation of and changes to the MFA solution via the customers' verified communication channel; and
   (c) deployment of MFA technology and channels that are more secure than unencrypted SMS.

6. A financial institution must ensure that the security controls of MFA solutions include adherence to the following requirements:
   (a) the MFA solution is resistant to interception or manipulation by any third party throughout the authentication process;
   (b) payer / sender must be made aware and prompted to confirm details of the identified beneficiary and amount of the transaction;
   (c) authentication code must be initiated and generated locally by the payer / sender using MFA;
   (d) authentication code generated by payer / sender must be specific to the confirmed identified beneficiary and amount;
   (e) secure underlying technology must be established to ensure the authentication code accepted by the financial institution corresponds to the confirmed transaction details; and
   (f) notification must be provided to the payer / sender of the transaction.

7. Where a financial institution deploys OTP as an additional factor of authentication, the following features must be implemented:
   (a) OTP must be dynamic where it changes each time it is required and time-bound;
   (b) binding of the transaction details to the OTP generated by the device (e.g. beneficiary account number, amount of transaction); and
   (c) generation of the OTP from the customer's device and not from the bank's server to mitigate the risk of manipulating OTP in the financial institution's infrastructure and increase customer control over authentication process.

8. Where a financial institution decides not to adopt MFA for financial transactions below RM10,000 to customer's own account, the financial institution must implement adequate safeguards to protect customer from digital fraud. This shall include-
   (a) SLA of T+3 calendar days (or less), T being the date of event reported by customer, for reversal of any unauthorised first-party transactions reported by customer;
   (b) set appropriate limits on a per-transaction basis, and on a cumulative basis;
   (c) provide a convenient means for customers to reduce the limits described in paragraph (b) or to opt for MFA; and
   (d) provide its customers with adequate notice of the safeguards set out in paragraphs (a) to (c).

9. A financial institution must offer to its customer a robust cryptographic key-based authentication[41] such as digital certificate or passwordless as an alternative to existing password based authentication method to mitigate the risk of credential of password being compromised or stolen. The enrolment of this method must be subject to robust verification and resilient against cyber threats and fraud techniques.

[41] Cryptographic-key-based authentication is a method used to verify the identity of a user or system through the use of cryptographic keys, typically involving a challenge-response handshake to prove one's identity.

Appendix 4 Control Measures for Mobile Applications and Devices

1. A financial institution that offers digital services must be aware of the risks associated with mobile applications. To mitigate these risks, a financial institution shall continuously assess and perform risk assessment to ensure that the threats associated with mobile applications is addressed.

2. A financial institution must ensure digital services involving sensitive customer and counterparty information offered via mobile devices are adequately secured. This includes the following:
   (a) design the mobile application to operate in a secure and tamper-proof environment[42] within the mobile devices to protect users against cyber threats such as malware and unauthorised access;
   (b) prohibit mobile applications from storing customer and counterparty information used for authentication with the application server such as PIN and passwords. Authentication and verification of unique key and PIN must be centralised at the host;
   (c) activation of the mobile application must be subject to robust authentication by the financial institution;
   (d) ensure secure provisioning and deprovisioning process of mobile application in the customer's device;
   (e) undertake proper due diligence processes to ensure the application distribution platforms used to distribute the mobile application are reputable;
   (f) ensure proper controls are in place to access, maintain and upload the mobile application on application distribution platforms; and
   (g) monitor the application distribution platforms to identify and address the distribution of fake applications in a timely manner.

3. A financial institution must also ensure the following measures are applied specifically for applications running on mobile devices used by the financial institution, appointed agents or intermediaries for the purpose of processing customer and counterparty information:
   (a) mobile device to be adequately hardened and secured;
   (b) ensure the capability to automatically wipe data stored in the mobile devices in the event the device is reported stolen or missing;
   (c) comply with industry standards processed in card payments to mitigate risks of unauthorised data access, identity theft and fraud[43];
   (d) enforce masking of sensitive customer and counterparty information when displayed on mobile devices; and
   (e) limit the storage of customer and counterparty information for soliciting insurance and takaful businesses in mobile devices to 30 days.

[42] Such as have not been compromised, jailbroken or rooted.
[43] This includes risks associated with malwares that enable keystroke logging, PIN harvesting and other malicious forms of customer and counterparty information downloading.

Appendix 5 Control Measures on Cybersecurity

A financial institution must adopt robust control measures to enhance its network resilience against cyber threats.

Part A: Network Security

1. A financial institution must ensure technology networks are segregated into multiple zones according to threat profile. Each zone shall be adequately protected by various security devices including but not limited to firewall and Intrusion Prevention System (IPS). This must include network for delivery of digital services and wireless networks as well.
2. A financial institution must ensure security controls for server-to-server external network connections include the following:
   (a) use PKI-based authentication method or equivalent alternatives;
   (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec; and
   (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus.
3. A financial institution must ensure security controls for remote access to server include the following:
   (a) restrict access to only hardened and locked down end-point devices;
   (b) use secure tunnels such as TLS and VPN IPSec;
   (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus;
   (d) close relevant ports immediately upon expiry of remote access; and
   (e) implement multi-factor authentication (MFA) for all remote access sessions.
4. A financial institution must ensure overall security controls are implemented including the following:
   (a) dedicated firewalls at all critical segments. All external-facing firewalls must be deployed on High Availability (HA) configuration and "fail-close" mode activated;
   (b) IPS at all critical network segments with the capability to inspect and monitor encrypted network traffic;
   (c) web and email filtering systems such as web-application firewalls, web-proxy, URL filtering, sandboxing features, spam filter and anti-spoofing controls;
   (d) end-point protection solution to detect and remove security threats such as malware;
   (e) enforce full hard disk encryption for all endpoints and systems;
   (f) solution to mitigate advanced persistent threats including zero-day and signatureless malware; and
   (g) capture the full network packets to rebuild relevant network sessions to aid forensics in the event of incidents.
5. A financial institution must synchronise and protect the Network Time Protocol (NTP) server against tampering.
6. A financial institution must ensure its technology systems and infrastructure, including critical systems outsourced to or hosted by third party service providers,

are adequately protected against all types of Distributed Denial of Service (DDoS) attacks (including Domain Name Service (DNS) based, volumetric, protocol and application layer attacks) through the following measures:

(a) subscribing to DDoS mitigation services, which include automatic 'clean pipe' services to filter and divert any potential malicious traffic away from the network bandwidth; and
(b) regularly assessing the capability of the provider to expand network bandwidth on-demand including upstream provider capability, adequacy of the provider's incident response plan and its responsiveness to an attack; and
(c) implementing geolocation controls based on customer profile location, trend or behaviours, in order to restrict access from unauthorised regions and reduce exposure to malicious traffic.

Part B: Data Security

1. A financial institution shall ensure that all data-at-rest of Personal Identifiable Information (PII) and transaction data are securely protected and rendered unreadable to unauthorised access through the implementation of robust encryption mechanisms or equivalent capabilities.

2. A financial institution must design internal control procedures and implement appropriate technology in all applications and access points to enforce Data Loss Prevention (DLP) policies and trigger any policy violations. The technology deployed must cover the following:
   (a) data in-use – data being processed by IT resources;
   (b) data in-motion – data being transmitted on the network; and
   (c) data at-rest – data stored in storage mediums such as servers, backup media and databases.

3. A financial institution must implement appropriate policies for the removal of data on technology equipment, mobile devices or storage media to prevent unauthorised access to data.

4. A financial institution must establish a clear DLP strategy and processes in order to ensure that proprietary and customer and counterparty information is identified, classified and secured. At a minimum, a financial institution must -
   (a) ensure that data owners are accountable and responsible for identifying and appropriately classifying data;
   (b) undertake a data discovery process prior to the development of a data classification scheme and data inventory; and
   (c) ensure that data accessible by third parties is clearly identified and policies must be implemented to safeguard and control third party access. This includes adequate contractual agreements to protect the interests of the financial institution and its customers.

5. A financial institution must ensure adequate security controls are in place to safeguard against customer information breach (CIB)[44], which include:

[44] This is also applicable to the financial institution intermediaries as well as their third party service providers.

(a) conducting continuous review to ensure that CIB does not occur in the IT environments of the financial institution, its intermediaries, or third party service providers. The financial institution shall also incorporate scanning or screening of customer information into the scope of periodic security assessments (e.g. penetration testing, red teaming, or other security validation exercises) to detect accidental exposure of customer information on financial institution's systems;
(b) enhancing cybersecurity operations to promptly detect and strengthen the safeguards against CIB;
(c) ensure that the scope of financial institutions' internal audit reviews encompasses the management and security controls pertaining to CIB; and
(d) conduct a thorough investigation to identify the technical root cause(s) of all CIBs with appropriate action and consequence management to mitigate recurrence.

Part C: Security Operations Centre (SOC)

1. A financial institution must ensure its SOC, has adequate capabilities for proactive monitoring of its technology security posture. This shall enable the financial institution to detect anomalous user or network activities, flag potential breaches and establish the appropriate response supported by skilled resources based on the level of complexity of the alerts. The outcome of the SOC activities shall also inform the financial institution's reviews of its cybersecurity posture and strategy.

2. The SOC must be able to perform the following functions:
   (a) adequate log collection and the implementation of an event correlation engine with parameter-driven use cases such as Security Information and Event Management (SIEM);
   (b) incident coordination and response;
   (c) vulnerability management;
   (d) threat hunting;
   (e) remediation functions including the ability to perform forensic artifact handling, malware and implant analysis;
   (f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations and monitoring Indicators of Compromise (IoCs). This includes advanced behavioural analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers; and
   (g) has a well-documented and standardized playbook that covers common and plausible cyber threat scenarios, such as ransomware attacks.

3. A financial institution must ensure that the SOC provides monthly threat assessment report, which shall include, at a minimum, the following:
   (a) trends and statistics of cyber events and incidents categorised by type of attacks, target and source IP addresses, location of data centres and criticality of applications; and
   (b) intelligence on emerging and potential threats including Tactics, Techniques and Procedures (TTP).

4. A financial institution must subscribe to reputable threat intelligence services to identify emerging cyber threats, uncover new cyber-attack techniques and support the implementation of countermeasures.

5. A financial institution must ensure the following:
   (a) the SOC is located in a physically secure environment with proper access controls;
   (b) the SOC operates on a 24x7 basis with disaster recovery capability to ensure continuous availability; and
   (c) the SOC has a holistic and end-to-end view of the financial institution's infrastructure including internal and external facing perimeters.

Part D: Vulnerability Assessment and Penetration Test (VAPT)

1. A financial institution must establish standard operating procedures (SOP) for VAPT activities to continuously identify vulnerabilities, assess potential risks and remediate the identified gaps. The SOP must outline the relevant control measures including but not limited to ensuring that the activities of external penetration testers are within the defined scope and are always subject to continuous oversight, validating the event logs and ensuring data purging.

2. A financial institution must perform a quarterly vulnerability assessment of external and internal network components that support all critical systems.

3. A financial institution must conduct annual intelligence-led penetration tests on its internal and external network infrastructure, critical systems as well as digital services including web, mobile and all external-facing applications. The test shall reflect extreme but plausible cyber-attack scenarios based on emerging and evolving threat scenarios. A financial institution must engage suitably accredited penetration testers and service providers to perform this function.

4. In addition to the periodic testing, a financial institution must also conduct intelligence-led penetration tests prior to introducing new systems for the new products or services to ensure the IT infrastructure is not accidently exposed due to unchecked network configuration.

5. A financial institution must ensure the outcome of the penetration testing exercise is properly documented and escalated in a timely manner to senior management to identify and monitor the implementation of relevant remedial actions.

6. A financial institution must undertake an independent compromise assessment on the technology infrastructure of its critical systems at least once every three years and ensure the results of such assessments are escalated to senior management and the board in a timely manner. The financial institution may leverage their group-level cyber risk management functions to support this requirement.

Part E: Application Programming Interface (API) Security

1. A financial institution must ensure that the level of API security implemented is commensurate with the potential risks involved. At a minimum, the financial institution is required to implement the following measures to mitigate cybersecurity risks associated with APIs:

   (a) implement and maintain a centralised API inventory. The inventory must comprehensively encompass identification, classification and prioritisation of all associated API connections and dependencies;
   (b) ensure availability of API service by designing APIs to be scalable for handling high level of traffic and implementing measures to mitigate denial of service attacks;
   (c) undertake secure coding practices during API development, which shall include but not be limited to validating security of third party code and libraries, implementing robust error handling, input validation and appropriate security headers;
   (d) employ robust encryption standards and effective key management controls;
   (e) deploy anti brute-force mechanisms, including but not limited to rate limiting, account lockout, and others;
   (f) implement strong and robust authorisation and authentication protocols that commensurate with the risks presented by the APIs;
   (g) consider utilizing an API gateway to manage access, authentication, and authorization of the APIs;
   (h) conduct periodic security assessments on APIs, including penetration testing and static / dynamic security testing;
   (i) continuous monitoring for APIs to ensure visibility into the utilization and performance of the APIs, for prompt identification and detection of potential suspicious activities; and
   (j) establish process to effectively revoke access token or API keys in the event of a compromise.

Appendix 6 Criteria for Simplified Notification for IT Services Enhancements

Guiding principles for simplified notification

1. Where the enhancement does not result in:
   (a) any introduction of new technology to the institution or industry;
   (b) any material changes in application architecture or network design (e.g. changes to cybersecurity tools, add-on features to existing digital services channel or existing approved platform such as loan applications, new non-complex activity e.g. chatbot); or
   (c) the transmission of confidential or sensitive data (e.g. motor underwriting engine by third party for calculation of motor premium).
2. Service expansion leveraging approved website / mobile application for digital services within financial group.
3. Integration with IT services operated by third party service providers that are subject to regulation by local or foreign authorities ("regulated entities").

Non-exhaustive list of technical arrangements for participation with regulated entities

(a) IT services operated by the Bank (e.g. RENTAS).

(b) IT services operated by institutions regulated by the Bank such as:
   (i) Payment services of approved payment system operators and registered merchant acquirers (e.g. Real-time Retail Payments Platform);
   (ii) Financial services operated by approved participants in the Financial Technology Regulatory Sandbox;
   (iii) Remittance services (e.g. by Western Union, Merchantrade, Paypal); and
   (iv) approved e-money issuers.

(c) Telecommunication services regulated by the Malaysian Communications and Multimedia Commission (MCMC).

(d) Participation in investment services and schemes regulated by local authorities:
   (i) Investment services approved by Securities Commission (e.g. Digital Investment Management);
   (ii) Regulated pilgrimage fund (e.g. Tabung Haji); or
   (iii) Approved investment funds (e.g. Amanah Saham National Berhad, Skim Simpanan Pendidikan Nasional).

(e) IT services provided by the Government of Malaysia, including those operated by the appointed third party service providers (e.g. e-invoicing by the Lembaga Hasil Dalan Negeri, MyEG, Financial Link, Rexit, Bestinet, etc).

(f) IT services provided by third party service providers regulated by international regulatory authorities e.g. SWIFT.

Appendix 7 Risk Assessment Report and Supervisory Expectations on External Party

Part A: Risk Assessment Report

Section 1: Financial Institution	
Name of Financial Institution	
Mailing address	
Type of digital services / cloud service / emerging technology	New / Enhancement
Description of the digital services / cloud service / emerging technology	
Key contact personnel	
Email address	
Phone number	
Section 2: External Service Provider	
Name of company	
SSM registration number	
Mailing address	
Engagement period	
Key contact personnel	
Email address	
Phone number	
Section 3: Detail of application	
Overview of the application i.e. business case, target segment of demographic and end-user, etc.	(Please keep the response below 200 words. Additional information may be provided as supporting documents)
Describe the technology used to support the product, service or solution	(Please keep the response below 200 words. Additional information may be provided as supporting documents)
Section 4: Technology risk assessment	

Technology risk assessment shall provide assurance on the effectiveness of technology risk control and mitigation performed by the financial institution in meeting expectations outlined in **Part D of this Appendix** and paragraph 17.1 (for cloud services and emerging technology).	
Section 5: Quality assurance	
Overall recommendation	
Section 6: Authorised signatory	
Signature	
Name	
Designation	
Date	

Part B: Format of Confirmation

Name of Financial Institution……

As Chairman of the board of directors / designated board-level committee / CISO / designated senior management officer * of [name of Financial Institution], I confirm that –

1. digital services / cloud service / emerging technology * is consistent with the bank's / insurer's / takaful operator's * strategic and business plans;
2. the board of directors / senior management * understand and are ready to assume the roles and responsibilities stated in Bank Negara Malaysia's policy document on Risk Management in Technology and are also apprised of all relevant provisions in the FSA, IFSA and DFIA and other relevant legislation, guidelines and codes of conduct;
3. risk management process related to digital services / cloud service / emerging technology * is subject to appropriate oversight by the board of directors and senior management;
4. appropriate security measures to address digital services / cloud service / emerging technology * security concerns are in place;
5. customer support services and education related to digital services / cloud service / emerging technology * are in place;
6. performance monitoring of digital services / cloud service / emerging technology * products, services, delivery channels and processes has been established;
7. digital services / cloud service / emerging technology * is included in the contingency and business resumption plans;
8. there are adequate resources to support the offering of digital services / cloud service / emerging technology * business; and
9. the systems, procedures, security measures, etc. relevant to sound operations of digital services / cloud service / emerging technology * will constantly be reviewed to keep up with the latest changes.

Signature : ……
Name : ……..
Date : ……..……..

* (*delete whichever is not applicable*)

Requirements on External Party Assurance

Part C: Financial Institutions are required to provide an external assurance

1. The assurance shall be conducted by an independent external service provider (ESP) engaged by the financial institution.
2. The independent ESP must understand the proposed services, the data flows, system architecture, connectivity as well as its dependencies.
3. The independent ESP shall review the comprehensiveness of the risk assessment performed by the financial institution and validate the adequacy of the control measures implemented or to be implemented.
4. The Risk Assessment Report (as per **Part D in Appendix 7**) shall state among others, the scope of review, risk assessment methodology, summary of findings and remedial actions (if any).
5. The Risk Assessment Report shall confirm there is no exception noted based on the prescribed risk areas (Negative attestation).
6. The financial institution shall provide the Risk Assessment Report accompanied by the relevant documents.

Part D: Minimum controls to be assessed by the independent External Service Provider, where applicable

1. The independent ESP assessment of security requirements shall include the following key areas:

   (a) access control;
   (b) physical and environmental security;
   (c) operations security;
   (d) communication security;
   (e) information security incident management; and
   (f) information security aspects of business continuity management.

2. For online transactions and services, a financial institution has implemented the following:
   (a) adequate measures to authenticate customer identity and ensure legitimate transaction authorisation by the customer, including-
      (i) measures to prevent session takeover or man-in-the-middle attacks;
      (ii) internal controls must be in place to prevent compromise of relevant internal systems / application / database;
      (iii) where appropriate, apply multi-level authentication, out of band protocol and real-time verification;
      (iv) secure session handling functions and authentication databases; and
      (v) ensure strong password and cryptographic implementation (recognised algorithm with reasonable key strength);

   (b) adequate measures for transaction authentication that promotes non-repudiation and establishes accountability-
      (i) mechanism exists to ensure proof of origin, content as well as the integrity of the message;
      (ii) chosen channel to deliver transaction is secure;

(iii) mechanism exists to alert the user on certain type of transactions for further authentication; and
(iv) establish mutual authentication or appropriate use of digital certification;

(c) segregation of duties and access control privilege for systems, databases and applications-
(i) implement dual control where applicable;
(ii) controls exist to detect and prevent unauthorised access to relevant resources / devices;
(iii) authorisation database must be tamper-resistant; and
(iv) periodic review of privileged users;

(d) adequate measures to protect data integrity of transactions and information:
(i) implementation of end-to-end encryption for external communication;
(ii) implementation of multi-layer network security and devices;
(iii) absence of single point of failures in network architecture;
(iv) conduct network security assessment / penetration test to identify vulnerabilities;
(v) establish audit trail capabilities;
(vi) preserve the confidentiality of information;
(vii) use of stronger authentication for higher risk transactions; and
(viii) timely notification to customers that is sufficiently descriptive of the nature of the transaction; and

(e) adequate measures to mitigate associated risks of using electronic mobile devices to perform online transactions, which shall include the following:
(i) application is running on secure mobile operating system versions;
(ii) application is not running on compromised devices;
(iii) conduct penetration test to identify and rectify potential vulnerability;
(iv) secure end-to-end communication between the device and host;
(v) sensitive information is not stored on mobile devices;
(vi) user is notified of successful transactions;
(vii) user is notified of suspicious transactions;
(viii) continuous monitoring and takedown of fake applications in application distribution platforms;
(ix) controls over the uploading of application-to-application distribution platforms;
(x) a unique code is generated per transaction; and
(xi) timely expiry of the transaction code.

Appendix 8 IT and Cyber Risks Associated with Third Party Service Providers

1. Operational performance and capacity (including staff competency and bench strength to mitigate key-man risks, system infrastructure reliability and IT operation management for service quality, strong recovery and resumption capability for business continuity).

2. Security requirements to mitigate information security risks relating to secure handling of confidential information pertaining to the financial institution, its customers or counterparty during transmission, process or storage of such information-

   (a) security governance;
   (b) IT asset management and protection against evolving cyber threats. This includes ensuring the storage of its data is at least logically segregated from the other clients of the third party service provider;
   (c) secure system development lifecycle;
   (d) physical security;
   (e) personnel security;
   (f) access management; and
   (g) incident management.

3. Cyber supply chain risks:

   (a) vetting of personnel;
   (b) vetting of third party or open source software and system interdependence;
   (c) third party risk management for key sub-contractors; and
   (d) concentration and geopolitical risk.

Appendix 9 Guidance on Emerging Technologies

1. As the landscape of emerging technology is dynamic and evolving, a financial institution shall ensure technology risk management framework (TRMF) is effective in monitoring the build-up of risks at the enterprise level arising from the use of new technologies. A financial institution shall provide clarity in its governance arrangement relating to new technologies as follows:
   (a) appropriate level of caution, factoring the unintended consequences such as fairness, ethics, legal liability exposures and frictions to vulnerable customers in the risk assessment and tolerance level;
   (b) acceptance criteria for introduction of new technology and reporting structure and oversight mechanism to uphold accountability throughout the lifecycle of adoption;
   (c) enhancement of technology and cybersecurity operation controls to mitigate attendant risks; and
   (d) evaluation and improvement of operating control effectiveness on on-going basis.

2. A financial institution must only allow the use of emerging technology in a production environment when, at a minimum, the following requirements are met:
   (a) IT system using the new technology is adequately tested to meet the service quality, resiliency, and information security objectives of the institution with residual risk that remains within the financial institution's risk tolerance level;
   (b) availability of industry standards and best practices to effectively test the operation risk controls and cyber defence. Where this cannot be met, additional margin of conservatism shall be applied in the risk assessment and the scope of provision to customers;
   (c) the financial institution must be prepared to suspend the use of emerging technology applications when extreme events such as adversarial attacks arise;
   (d) the financial institution must implement regular monitoring to assess consistency in the quality of the solution, security and compliance, enabling timely identification and mitigation to any emerging risks or issues; and
   (e) the financial institution must disclose to users that emerging technology is utilized in the system, providing adequate information about associated risks to enable them to make an informed decision before using the service.

Appendix 10 Key Risks and Control Measures for Cloud Services

This appendix provides additional guidance to financial institutions for the assessment of common key risks and considerations of control measures when financial institutions adopt public cloud for critical systems. The guidance is broadly applicable across various cloud service models and financial institutions is expected to apply a risk-based approach in implementing the guidance.

The guidance consists of two (2) parts:

- **Part A: Cloud governance** – describes the considerations governing the cloud usage policy, and technology skills capacity to implement cloud services securely and effectively.
- **Part B: Cloud design and control** – describes the considerations related to designing robust cloud infrastructure and in operationalising the cloud environment. This places emphasis on cloud architecture, cloud application delivery model, high velocity software development, user access management, data protection, key management, cloud backup and recovery, business continuity management and cybersecurity management.

Part A: Cloud Governance

A financial institution should ensure robust cloud governance processes are established prior to cloud adoption and are subject to on-going review and continuous improvement. This should cover the following areas:

1. Cloud risk management

(a) The board of a financial institution is expected to promote and implement sound governance principles throughout the cloud service lifecycle in line with the financial institution's risk appetite to ensure safety and soundness of the financial institution.

(b) The senior management of a financial institution is expected to develop and implement a cloud risk management framework that integrates with existing outsourcing risk management framework, technology risk management framework (TRMF) and cyber resilience framework (CRF), for the board's approval, proportionate to the materiality of cloud adoption in its business strategy, to assist in the identification, monitoring and mitigating of risks arising from cloud adoption.

(c) Common cloud service models[45] are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), wherein each presents a different set of capabilities offered to the financial institution as the cloud consumer, and hence a different set of shared responsibilities. In view of this, the cloud risk management framework of the financial institution should:

[45] Cloud service models consist of SaaS, PaaS and IaaS. Refer the Special Publication 800-145 on Definition of Cloud Computing issued by the National Institute of Standards and Technology, U.S. Department of Commerce.

i) be an integral part of the financial institution's enterprise risk management framework (ERM);
ii) be tailored to the cloud service models, both currently in use or being considered for use; and
iii) specify the scope of the financial institution's responsibility under each shared responsibility model, as the associated risks may vary.

(d) A financial institution is responsible for the protection of data stored in cloud irrespective of cloud service models and the cloud service providers. Therefore, the financial institution's understanding of the specific details of the cloud arrangement, particularly what is or is not specified in the terms of the contract with the cloud service providers is essential.

(e) Regardless of the cloud arrangement with cloud service providers, the onus remains on the financial institution to satisfy the Bank that it is protecting customer information and ensuring service reliability.

(f) The use of cloud services may represent a paradigm shift in technology operation management as compared to on-premises IT infrastructure. Business processes may change and internal controls on compliance, business continuity, information and data security may be overlooked due to the ease of subscribing to cloud services. Therefore, the cloud risk management framework should also clearly articulate the accountability of the financial institution's board and senior management, and the process involved in approving and managing cloud service usage, including the responsibility of key functions across the enterprise in business, IT, finance, legal, compliance and audit, over the lifecycle of cloud service adoption.

(g) As the cloud landscape rapidly evolves, a financial institution`s cloud risk management framework should undergo periodic review (at least once every three years to ensure its adequacy and effectiveness to manage new service models over time), or immediately upon any major cybersecurity incidents involving the cloud services.

2. Cloud usage policy

(a) The financial institution's senior management is expected to develop and implement internal policies and procedures that articulate the criteria for permitting or prohibiting the hosting of information assets on cloud services, commensurate with the level of criticality of the information asset and the capabilities of the financial institution to effectively manage the risks associated with the cloud arrangement.

(b) A financial institution is expected to expand the scope of its current technology assets inventory to include critical systems hosted on the cloud services, with a clear assignment of ownership, and to be updated upon deployment and changes of IT assets to facilitate timely recalibration of cybersecurity posture in tandem with an evolving threat landscape. Having visibility on the latest view of

the technology asset would enable effective triaging, escalation and response to information security incidents.

(c) A financial institution should regularly review and update the cloud usage policy at least once every three years. However, where any material changes arise, including but not limited to adoption of new cloud service deployment model, or adoption of cloud service for IT systems with higher degree of criticality, the financial institution should review and update its cloud usage policy immediately.

3. Due diligence

Due diligence on the prospective cloud service providers should be risk-based and conducted to a level of scrutiny that is commensurate with the criticality of the information and technology assets to be hosted on the cloud in compliance with relevant requirements and guidance as stipulated in the Third Party Service Provider Management section of this policy document and paragraphs 9, 10 and 11 in the Bank's Outsourcing policy document (Outsourcing process and management of risks, Outsourcing outside Malaysia, Outsourcing involving cloud services).[46]

4. Access to cloud service providers' certifications

A financial institution should review their cloud service providers' certifications prior to entering into any cloud arrangement or contract with such cloud service providers. At a minimum, a financial institution should:

(a) Seek assurance that the cloud service provider continues to be compliant with relevant legal, or regulatory requirements as well as contractual obligations and assess the cloud service provider's action plans for mitigating any non-compliance; and

(b) Obtain and refer to credible independent external party reports of the cloud platforms when conducting risk assessments. The financial institution's risk assessment should address all the requirements and guidance as stipulated in the Cloud Services section of this policy document and paragraph 11 of the Bank's policy document on Outsourcing which sets out provisions on outsourcing involving cloud services.

5. Contract management

A financial institution should set out clearly and where relevant, measurable, contractually agreed terms and parameters on the information security and operational standards expected of the cloud service providers. Such contract terms and parameters should be aligned with the financial institution's business strategy, information security policies and regulatory requirements.

[46] Or the relevant paragraphs in the policy documents applicable for eligible e-money issuer, non-bank registered merchant acquirer, intermediary remittance institution and operator of designated payment system.

(a) The terms of the contracts between the financial institution and cloud service providers should address the risks associated with cloud services and third party service providers;

(b) Jurisdiction risk may arise because cloud service providers operate regionally or globally in nature and may be subject to the laws and regulatory requirements of its home country, the location of incorporation, and the country where the client receives the service. Therefore, a financial institution should:

  i) identify and address potential jurisdiction risks by adopting appropriate mitigating measures, where practically possible, to ensure the use of cloud services does not impair its ability to comply with local law and regulatory requirements; and

  ii) understand the scope of local customer protection legislation and regulatory requirements as well as to ensure that the financial institution receives adequate protection and recourse for the benefit of its customers, in the event of a data breach or fulfilment of a legal data request by the cloud service provider;

(c) A financial institution should assess the potential impact and formalise arrangements with cloud service providers to comply with local laws and regulatory requirements for incident investigation and law enforcement purposes. This would include adhering to data retention requirements and data access procedural arrangements to ensure the confidentiality and privacy of the customers are protected; and

(d) The provision of cloud services by the primary cloud service provider may interconnect with multiple layers of other fourth party service providers (such as sub-contractors), which could change rapidly. For example, customer data could be leaked due to exposure caused by fourth party service providers. To mitigate the risks associated with such fourth party service providers, financial institutions should:

  (i) understand the scope of customer information shared across the supply chain and ensure that relevant information security controls can be legally enforced by the financial institution; and

  (ii) ensure Service Level Agreement (SLA) negotiations and contractual terms cover the performance matrix, availability, and reliability of services in order to ensure that the cloud service providers agree and are formally aligned on the requirements and standard of cloud services provided. In addition, cloud service providers should be accountable to the financial institution for the SLA, performance matrix, availability and reliability of cloud services rendered by its service providers (i.e. sub-contractors).

6. Oversight over cloud service providers

A financial institution should ensure effective oversight over cloud service providers taking into account the fact that the cloud service providers may engage sub-contractor(s) to provide cloud services. This includes, at a minimum, the following:

(a) establish and define a continuous monitoring mechanism with alignment to the enterprise outsourcing risk management framework (or equivalent) to ensure

adherence to the agreed SLA, compliance of the cloud service provider with any applicable legal and regulatory requirements and resilience of outsourced technology services on on-going basis;

(b) identify, assign and document the key responsibilities within the financial institution for continuous monitoring of cloud service providers to ensure accountabilities are clearly defined;

(c) perform assessments of the outsourcing arrangement involving cloud service providers periodically in accordance with the financial institution's internal policy to achieve business resilience with emphasis on data security and ensure prompt notification to the Bank of the developments that may result in material impact to the financial institution (such as jurisdiction risks for data hosted overseas due to evolving foreign legislation and geopolitical development) in line with the Bank's policy document on Outsourcing, in particular, provisions relating to outsourcing of cloud services outside Malaysia including paragraphs 9, 10 and 11 of the Outsourcing policy document; and

(d) promptly review or re-perform risk assessment upon any material changes in cloud risk profile such as jurisdiction risks for data hosted overseas due to evolving foreign legislation and geopolitical development.

7. Skilled personnel with knowledge on cloud services

(a) The adoption of cloud services requires commensurate changes to the financial institution's internal resources and process capabilities. In this regard, a financial institution should:

  i) equip its board and senior management with appropriate knowledge to conduct effective oversight over the cloud adoption; and

  ii) ensure its IT and security operations or relevant personnel are appropriately skilled in the areas of cloud design, migration, security configurations, including administrative, monitoring and incident response;

(b) The effective management of cloud services is not purely the responsibility of the financial institution's IT function. Therefore, a financial institution should ensure relevant internal resources in business operations, finance, procurement, legal, risk and compliance are also adequately skilled and engaged to manage the change in risk profile arising from cloud adoption. This should also enable financial institutions to respond effectively to operational incidents;

(c) A financial institution should equip internal audit and personnel undertaking the risk management and compliance functions with relevant cloud computing and cloud security skills to be able to verify the effectiveness of the information security controls in alignment with the financial institution's cloud usage policy and information security objectives;

(d) A financial institution should ensure that its staff receive adequate training to understand their responsibilities in complying with internal cloud usage policies and are prepared to effectively respond to a range of security incident scenarios developed on a risk-based approach; and

(e) A financial institution should expand the scope of the formal consequence management process to govern the use of cloud services to ensure the cloud usage policy is effectively enforced given that cyber hygiene is critical to ensure the continued security of cloud service usage.

Part B: Cloud Design and Control

A financial institution should design its adoption of cloud services with a degree of portability, scalability and fault tolerance that is proportionate to the materiality of the cloud service to its business operation. It should also ensure robust operational controls are in place to manage its ongoing cloud operations.

1. Cloud architecture

(a) A financial institution should design a robust cloud architecture and ensure such design is in accordance with the relevant international standards for the intended application.

(b) A financial institution is encouraged to adopt zero-trust principles to provide a cyber resilient architecture by adopting an “assume breach” mindset, layering defense-in-depth through micro-segmentation, “deny-by-default”, “least privilege” access rights, and conducting deep inspection and continuous validation where applicable.

(c) A financial institution should use the latest network architecture approach and appropriate network design concept and solutions for managing and monitoring granular network security and centralised network provision in managing complexity of the cloud network environment.

(d) A financial institution should establish and utilise secure and encrypted communication channels for migrating physical servers, applications, or data to the cloud platforms.

(e) For financial institutions leveraging on their financial group’s cloud infrastructure, the financial institutions should consider an appropriate level of network segregation (e.g. logical tenant isolation in the shared environment of the cloud) to mitigate the risk of cyber-attacks from propagating cross-border or cross-entity and affecting the Malaysian financial institution’s operations.

(f) The increasing use of application programming interfaces (API) by financial institution to interconnect with external application service providers could achieve efficiency in new service delivery. However, this may increase the cyber-attack surface, and any mismanagement may amplify the impact of an information security incident. A financial institution should ensure its APIs are subject to rigorous management and control mechanisms which include the following:

    i) APIs should be designed for service resilience to avoid the risk of single points of failure and configured securely with appropriate access controls; and

    ii) APIs should be tracked and monitored against cyber-attacks with adequate incident response measures and are de-commissioned on a timely basis when no longer in use.

2. Cloud application delivery models

(a) Cloud application delivery models may evolve to support faster time-to-market in response to consumer demand. Currently, DevOps and Continuous Integration/Continuous Development (CI/CD)[47] are amongst the prevailing practices and processes for cloud application delivery. For instance, the ability to enforce segregation of duties for CI/CD where application developers may require access to the management plane for service configuration. A financial institution should ensure CI/CD pipelines are configured properly to enhance security of automated deployments and immutable infrastructure[48].

(b) A financial institution should continuously leverage enhanced cloud capabilities to improve the security of the cloud services and financial institutions are, among others, encouraged to-

i) adopt industry best practices such as infrastructure-as-code (IaC)[49] to automate the provisioning of IT infrastructure in a consistent, scalable and secure manner; and

ii) use immutable infrastructure practices for deployment of services to reduce the risk of failure by creating a new environment with the latest stable version of the software. The on-going monitoring of the cloud environment should include automating the detection of changes to immutable infrastructure to improve compliance review and combat evolving cyber-attacks.

(c) Where relevant, a financial institution should implement appropriate controls on the IaC process to minimise the risk of misconfiguration and reduce the cyber-attack surface. This includes the following measures that should be taken by the financial institution:

i) conduct vulnerabilities scanning as part of IaC automation steps and ensure issues are remediated prior to the provisioning of IT infrastructure;

ii) ensure virtual machine images (VMI) or container images of IaC templates are trusted and digitally signed; and

iii) implement appropriate access control to prevent unauthorised changes to IaC templates.

3. Virtualization and containerization management

The guidance provided in this paragraph is applicable to financial institutions which use or plan to use PaaS and IaaS cloud service models only.

[47] CI/CD is a set of methods that enables developers to deliver code changes more frequently using automation.

[48] Immutable infrastructure is an approach to managing and deploying infrastructure where components, such as virtual servers and networks, are created once and then never modified. If a new version of a service or application requires changes to the underlying infrastructure components, new instances of those components are created and the old instances are replaced.

[49] The process of managing and provisioning an organization's IT infrastructure using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools - NIST Special Publication 800-172, U.S. Department of Commerce, February 2020.

(a) A financial institution should ensure virtualization services are configured in line with the prevailing guidance from the cloud service providers and industry best practices, commensurate with the evolution of cloud computing technologies.
(b) A financial institution should ensure virtual machine and container images are configured, hardened, and monitored appropriately. This includes the following:
    i) use stable images and keep images up to date;
    ii) store and use images from trusted repositories or registries;
    iii) scan images for vulnerabilities, remediate any vulnerabilities prior running in production;
    iv) enforce “least privilege” access;
    v) harden images based on industry best practices; and
    vi) stored images are subjected to security monitoring from unauthorised access and changes.

4. Change management

(a) A financial institution should establish a process to systematically assess and take appropriate action to manage the impact of the releases by cloud service providers in relation to existing infrastructure, network, upstream and downstream systems to minimize the impact of any service disruption.
(b) A financial institution should ensure its existing change management process is extended to cover cloud services where appropriate to promote effective and secure system development. The escalation process and approving authority should be clearly defined to ensure critical changes can be implemented and risk of service disruptions are mitigated promptly.
(c) All critical changes deployed to the production environment should also be timely applied across environments such as disaster recovery site or supported cloud regions and availability zones where appropriate.

5. Cloud backup and recovery

(a) As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following:
    i) define and formalise backup and recovery strategy at the planning stage of cloud adoption;
    ii) conduct periodic reviews of the cloud service providers’ restoration and recovery capabilities; and
    iii) conduct testing of recovery strategy prior to deployment of the system.
(b) A financial institution should ensure backup and restoration procedures are periodically tested to validate recovery capabilities. The frequency of backup procedures should be commensurate with the criticality of the system and recovery point objective (RPO) of the system. Remedial actions should be taken promptly by the financial institution for unsuccessful backups.

(c) A financial institution should ensure sufficient backup and recovery of virtual machine and container including backup configuration settings (for IaaS and PaaS, where relevant), which includes the following:
   i) ensure the capability to restore a virtual machine and container at point-in-time[50] as per the business recovery objectives; and
   ii) make virtual machine and container images available in a way that would allow the financial institution to replicate those images at alternate sites or recovery sites[51];

(d) A financial institution should assess the resilience requirements of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availability in the extreme adverse scenarios. The financial institution should consider a risk-based approach and progressively adopt appropriate mitigating controls to ensure service availability and mitigate concentration risk. Amongst the viable options are:
   i) leverage cloud services' high availability and redundancy features to ensure production data centres have redundant capacity in different availability zones;
   ii) achieve geographical redundancy by having data centres in different geographical regions;
   iii) adopt hybrid cloud (combination of on-premises and public cloud setup);
   iv) establish back-up cloud service providers and identify appropriate arrangement for porting of data and application to ensure timely service resumption; and
   v) adopt multi-cloud strategy, with the use of services from different cloud service providers to mitigate concentration risks and geopolitical risks.

6. Interoperability and Portability

Interoperability standards for cloud services continue to evolve such that porting data, related configuration and security logging across different cloud service providers may be challenging. To facilitate the smooth process of interoperability and portability between on-premise IT systems or alternate cloud service providers, financial institutions are encouraged to-

(a) assess technical requirements for interoperability and portability prior to entering into an agreement or arrangement with the cloud service providers to avoid vendor lock-in;

(b) maintain a list of third party service providers and tools that are needed to facilitate a smooth transition;

(c) ensure usage of standardized network and communication protocols for ease of interoperability and portability with on-premise IT systems or alternate cloud platforms;

[50] Point-in-time refers to the ability to preserve and retrieve the state of a virtual machine or system at a specific moment.

[51] The alternate sites and recovery sites could either be in-house arrangements, or available through agreement with third party recovery facility provider, or a combination of both options.

(d) ensure the use of common electronic data formats, where applicable, to ease the movement of data between cloud service providers or to on-premises IT system; and
(e) extend patch and EOL management to ensure technology solutions employed remain effective and protected against system vulnerabilities.

7. Exit strategy

(a) A financial institution should establish a robust cloud exit strategy as part of its cloud risk management framework to prepare for extreme adverse events such as the unplanned failure or termination of cloud service providers. The exit strategy should:
    i) be developed during the cloud deployment planning phase rather than on an ex-post basis;
    ii) identify alternative cloud service providers (multi-cloud approach) or third party solutions, or other such means to ensure no business recovery objectives disruption or vendor lock-in;
    iii) be properly documented including details on the various exit trigger scenarios, roles and responsibilities, and sufficient resources to manage exit plans and the transition activities; and
    iv) be updated in a timely manner to reflect any material developments.

(b) A financial institution's exit strategy should be supported by an appropriate and proportionate exit plan that establishes the operational arrangements to facilitate an orderly exit from an agreement or arrangement with cloud service provider, including the following:
    i) conduct impact assessment to determine potential costs, resources, and timing implications of transferring cloud services to an alternative cloud service providers or rely on the in-house arrangement at the financial institution;
    ii) identify appropriate methods to port data and applications to an alternative arrangement;
    iii) to obtain written confirmation or attestation from the cloud service providers or independent external service providers that all sensitive data has been securely deleted from the cloud service provider's system upon completion of the exit process; and
    iv) conduct testing to validate the effectiveness of the exit plan, to obtain a reasonable degree of assurance of its effectiveness.

8. Cryptographic key management

(a) A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud.

(b) A financial institution should ensure its policies and procedures on cryptography are extended to cover cloud services where relevant, to promote the adoption of strong cryptographic controls.

(c) Where appropriate and feasible, financial institutions should retain ownership and control of the encryption keys (themselves or with an independent key custodian), independent from the cloud service provider, to minimize the risk of unauthorised access to the data hosted on the cloud.

(d) As the usage of cloud adoption increases, managing many encryption keys used for protecting data has become more complex and may introduce new challenges for financial institutions. A financial institution should adopt a comprehensive and centralised approach to key management including the use of centralised key management system that can handle generations, storage and distribution of keys in a secure and scalable manner.

9. Access Controls

(a) The management plane is a key security difference between traditional infrastructure and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deployment. In view of this, financial Institutions should ensure the use of strong controls for accessing the management plane which may include the following:

i) allocate dedicated and effectively hardened endpoints and up to date patching of software to access the management plane;

ii) implement “least privilege” and strong multi-factor authentication (MFA) e.g. strong password, soft token, privileged access management tool and maker-checker functions;

iii) employ granular entitlement allocation for privileged users;

iv) conduct continuous monitoring of the activities performed by privileged users; and

v) ensure secure communication protocols are in place for accessing the management plane. e.g. secure end-to-end communication channels, whitelisting of IP addresses, etc.

(b) A financial institution should extend its user access matrix to cover user access rights for both the financial institution and its cloud service providers where relevant for the ongoing access to cloud services.

(c) A financial institution should ensure their tenant access controls to all hypervisor management functions or administrative consoles for systems hosting virtualized systems are effectively implemented in accordance with the requirements and guidance under the Access Control section of this policy

document. These controls should mitigate the risk of any unauthorised access to the hypervisor management functions and virtual machine.

(d) Point-to-point connections with cloud services may proliferate with the ease of cloud adoption, resulting in fragmentation of identity and access management and the risk of unsanctioned data being migrated to the cloud. In view of this, rigorous planning is recommended for the design of identity and access management as it is inherently complex. Financial institutions are encouraged to:

i) where appropriate and commensurate with the size and complexity of the cloud adoption, implement a federated[52] approach for identity and access management to mitigate risks of identities in cloud services being disjointed from the internal identities, unauthorised access and to ease user access management; and

ii) consider additional attributes in context-aware decisions for identity and access management such as pattern of access to further mitigate the risks associated with remote access.

10. Cybersecurity Operations

(a) A financial institution should ensure the governance and management of cybersecurity operations is extended to cover cloud services, with appropriate control measures to prevent, detect, and respond to cyber incidents in the cloud environment to maintain the overall security posture of the institution.

(b) The interconnected cloud service supply chain could become a source of cyber risk. A financial institution should ensure integrated monitoring and full visibility of cloud services are established. This should include the following:

i) continuous monitoring of system communications between the cloud service provider, on-premise IT systems and other service providers to ensure the security perimeter is not breached; and

ii) ensuring that third party service providers, including those providing ancillary functions, have adequate capabilities to monitor, detect and respond to anomalous activities, with timely communication to the financial institution of relevant cyber incidents.

(c) A financial institution should understand the segregation of responsibility in security management, which varies across the cloud service models. A financial institution should manage the sources of vulnerabilities appropriately including by:

i) proactively seeking assurance of their cloud service providers to conduct periodic VAPT on the cloud infrastructure to ensure tenant isolation and overall security posture remains healthy; and

ii) understanding the cloud service provider's VAPT policy for the financial institution on cloud infrastructure for IaaS model given the varying degree

[52] Federated approach for identity and access management is a process / arrangement between multiple systems or enterprises that enables users to use the same identification data to access all related networks.

of the financial institution's access to the cloud environment and establish a VAPT arrangement with cloud service providers upfront which commensurate with the complexity of the cloud environment.

11. Distributed Denial of Service (DDoS)

(a) A financial institution should ensure that its DDoS mitigation service is commensurate with the size and complexity of the cloud adoption.

(b) The risk of a single point of failure may surface when a financial institution leverages solely on a cloud-based solution to mitigate DDoS attacks. As such, a financial institution is encouraged to engage alternative DDOS mitigation providers or establish circuit breakers to avoid service disruption when the main DDOS mitigation provider is disrupted.

12. Data Loss Prevention (DLP)

(a) A financial institution should protect the data hosted in cloud services as required under the Data Security of **Appendix 5** of this policy document, including the expansion of the endpoint footprint if the financial institution allows its staff to use their own devices to access the sensitive data.

(b) As it becomes increasingly easy to distribute digital content to customers via cloud services, a financial institution should adopt the appropriate digital rights management mechanism to preserve the confidentiality of its proprietary and customer information.

13. Security Operations Centre (SOC)

(a) A financial institution should understand the scope of cloud service providers' responsibility for cybersecurity monitoring and adapt its SOC strategy and processes to ensure proactive and holistic monitoring of its cybersecurity posture. This adaptation should include the ability to effectively improve cybersecurity telemetry and analysis to detect and respond to cyber threats.

(b) Where applicable, the responsibilities of cloud service providers with respect to SOC operations should be formalised in the agreement or arrangement between the financial institution and the cloud service providers, including the retention period required for relevant logs needed for forensic purposes and the right of the financial institution to access the logs for quick restoration as and when needed, in accordance with the requirements and guidance under the Access Control section and Part C of **Appendix 5** of this policy document.

14. Cyber response and recovery

(a) A financial institution should enhance existing cyber crisis management policies and procedures to remain in a state of readiness to respond to cyber threats in a cloud environment.

(b) A financial institution should extend its Cyber Incident Response Plan (CIRP) to include adverse scenarios that may affect cloud services and establish clear

roles and responsibilities between the financial institution and cloud service providers for incident response and remediation. The incident escalation process and turnaround time should be established with cloud service providers and periodically reviewed, to achieve an effective incident response.

(c) A financial institution should consider the following additional measures in the development of its CIRP:
   i) enhance its ability to detect security breach incidents to achieve effective incident management, including the ability to detect data leakage on the dark web;
   ii) provide adequate assistance to customers in the event of a security breach in view that the complexity of cloud arrangements and sophistication of cyber-attacks often exceed the response range reasonably expected of customers; and
   iii) ensure CIRP is ready to manage cross-border incidents where the data resides in a foreign jurisdiction.

(d) A financial institution should ensure that relevant Cyber Emergency Response Team (CERT) members are conversant with the CIRP covering cloud services to effectively activate the CIRP when incidents occur.

(e) A financial institution should extend its existing incident reporting requirements to include cloud services.

(f) A financial institution should enter into agreements or arrangements with its cloud service providers to conduct integrated business continuity testing and cyber drill in accordance with the requirement on testing of disaster recovery plan in paragraph 9.48 and 9.50 of the Bank's policy document on Business Continuity Management (BCM) and paragraphs relating to cyber response and recovery under this policy document to test the effectiveness of the financial institution's CIRP and recovery plan.

(g) A financial institution should review its loss provision arrangements to ensure its adequacy to cover cyber incidents in accordance with the requirement on paragraph 11.17 of this policy document.

Appendix 11 Fraud Detection Standards

A financial institution is required to adhere to the specified requirements, which include carrying out financial transactions conducted via digital services for retail customer.

While compliance with the minimum standards is essential, a financial institution is encouraged to exceed these standards to stay ahead of emerging threat. The financial institution shall continuously upgrade and refine their fraud detection capability to ensure it remains robust against the anticipated level of threat.

1. A financial institution must establish detailed and comprehensive risk profiles for each customer as a reference point when performing fraud detection based on behavioural analysis of the financial institution's customer and fraud profiles. Examples of relevant factors to be considered may include:
   (a) demographics information e.g. age, gender, race, occupation, salary, language, etc;
   (b) geographical information e.g. city, state, countries, IP address;
   (c) historical transactional patterns e.g. monetary transfer amount, time of transaction, velocity, new beneficiaries / favourite transfer; and
   (d) behavioural patterns e.g. time taken to make transfer, typing speed, mouse hovering pattern.

2. A financial institution must be able to detect and block suspicious or fraudulent transactions on a real-time basis based on individual customer risk profiles established in accordance with paragraph 1 through the fraud risk analytics. At minimum, the fraud risk analytics must include the parameters or indicators outlined below:
   (a) Access to or conduct of a deposit account by a customer for a period of time following specific activities which could indicate elevated risk of identity theft or fraud, such as:
      i) newly enrolled e-banking account;
      ii) activation of online banking access for existing customer;
      iii) registration of multi-factor authentication (MFA) method on a new device;
      iv) increase in transaction limit;
      v) password reset;
      vi) change of personal information such as phone number, email, and postal address;
      vii) registration of third party payee details (favourite accounts); and
      viii) upliftment of fixed deposit accounts or linked investment / unit trust accounts.

   (b) Transaction patterns observed in a customer's account, which could indicate elevated risk of identity theft or fraud, such as:
      i) high volume of debits in a short period to new beneficiaries within a day or next few days following such activities as specified in 2(a).
      ii) sudden change in transaction patterns (e.g. increases in frequency or cumulative value over a short period, or large withdrawals

resulting in low account balance inconsistent with the customer's normal transaction patterns);

iii) activities that may be inconsistent with the customer's risk profile or history (e.g. transaction time, high debits from a previously inactive account);

iv) large deposit made into a newly opened deposit account and withdrawn in a short period (e.g. within a few days);

v) transactions initiated from an unusual geographical location (not the customer's typical location) or consecutive transactions from different locations within a short period of time;

vi) transactions initiated from an account or device previously reported for fraud by various sources of fraud intelligence (e.g. upon investigation by any financial institution, report from customer or law enforcement agencies, industry threat intel sharing, etc.);

vii) transactions from an account previously inactive for a period of time; and

viii) transactions to suspected financial mules detected by the financial institution or any other fraud repositories developed by the Bank, the industry, or law enforcement agencies.

(c) Changes in a device fingerprint, such as the location, IP address, device MAC, operating system and other device profile. This must include the ability to detect and block attempts to defeat or bypass device fingerprinting methodologies.

(d) Account takeover and identity fraud using advanced artificial intelligence tools, techniques, and procedures to defeat or bypass the authentication controls of digital services or contact centre.

(e) Higher risk scoring must be applied for vulnerable customers (e.g. senior citizens, younger customers, previous victims of fraud, customers with lower literacy on the safety of electronic banking or awareness level, etc).

(f) Changes in biometric credentials registered in a device, where biometric technologies are solely used for financial transaction authentication purposes. This includes the scenario where a mobile banking application relies on the biometric verification function of the device, mobile operating system, or a third party application.

3. A financial institution must implement measures to promptly detect and terminate hijacked sessions to prevent unauthorised access to customer accounts. The financial institution shall notify customer on elevated cyber risk caused by the presence of risky application (e.g. application downloaded outside official distribution platforms or detected to contain security vulnerabilities).

4. When customer' online banking access is restricted, a financial institution must promptly notify customer with appropriate guidance to enable customer to restore access to their account subject to robust verification. To mitigate privacy

concerns, the financial institution must seek consent from the customer prior to effecting the customer device profiling.

5. A financial institution must investigate suspicious transactions based on pre-determined priority levels and conduct the necessary verification (such as call-backs or other effective methods) with the customer prior to releasing any flagged transactions. To ensure acceptable customer experience, the financial institution must notify the affected customer immediately upon the blocking of each suspicious transaction (e.g. via SMS or secure app notification) and deploy sufficient resources to contact the affected customer within 30 minutes of the transaction, including during peak periods. The verification procedures must consider and include ways to help detect circumstances where customer may be responding under the influence or threat of fraudsters. The financial institution must also establish a robust process to minimise risk in the event the customer cannot be contacted due to their unavailability.

6. A financial institution must ensure that its various touch points such as contact centres and branches are easily accessible and sufficiently resourced to provide customer with prompt advice or to connect customer with the fraud investigation team, if necessary.

7. A financial institution must continuously update its system to ensure fraud detection rules remain effective to combat new fraud modus operandi via the following:
   (a) enhance its fraud detection rules promptly upon detection of new fraud techniques that have evaded its fraud detection system. The enhancements shall be timely upon being notified by its internal fraud team or upon receiving such intelligence from external sources such as other financial institution, industry group, public-private partnership and other intelligence sharing platform; and
   (b) review the effectiveness of its fraud detection parameters and thresholds in a timely manner, taking into consideration recent typologies in relation to fraudulent transactions and financial mule accounts, including new digital fraud techniques and modus operandi in other jurisdictions.

8. In order to effectively address the wide range of fraud alerts that can arise from various fraud modus operandi and techniques, it is important to have clear and detailed procedures for managing suspected fraud cases. Therefore, the financial institution must develop a comprehensive fraud management playbook, as a point of reference for the relevant staff to promptly identify, confirm, and respond effectively to various scenarios. The playbook must be updated and validated at least once a year, or more frequently if needed, to ensure it remains relevant in the evolving fraud landscape. This includes reflecting insights from assessments of confirmed fraud cases and lessons learnt from incidences in which the financial institution was unable to detect the fraudulent activities or transactions.