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 issuer of electronic money
8. Operator of a designated payment system

Issued on: 19 June 2020 BNM/RH/PD 028-98

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 Technology risk refers to risks emanating from the use of information technology (IT) and the Internet. These risks arise from failures or breaches of IT systems, applications, platforms or infrastructure, which could result in financial loss, disruptions in financial services or operations, or reputational harm to a financial institution.

1.2 With the more prevalent use of technology in the provision of financial services, there is a need for financial institutions to strengthen their technology resilience against operational disruptions to maintain confidence in the financial system. The growing sophistication of cyber threats also calls for the increased vigilance and capability of financial institutions to respond to emerging threats. Critically, this should ensure the continuous availability of essential financial services to customers and adequate protection of customer data.

1.3 This policy document sets out the Bank's requirements with regard to financial institutions' management of technology risk. In complying with these requirements, a financial institution shall have regard to the size and complexity of its operations. Accordingly, larger and more complex financial institutions are expected to demonstrate risk management practices and controls that are commensurate with the increased technology risk exposure of the institution. In addition, all financial institutions shall observe minimum prescribed standards in this policy document to prevent the exploitation of weak links in interconnected networks and systems that may cause detriment to other financial institutions and the wider financial system. The control measures set out in Appendices 1 to 5 serve as a guide for sound practices in defined areas. Financial institutions should be prepared to explain alternative risk management practices that depart from the control measures outlined in the Appendices and demonstrate their effectiveness in addressing the financial institution's technology risk exposure.

2 Applicability

2.1 This policy document is applicable to all financial institutions as defined in paragraph 5.2.

3 Legal provision

3.1 The requirements in this policy document are specified pursuant to—

(a) Sections 47(1) and 143(2) of the Financial Services Act 2013 (FSA);
(b) Sections 57(1) and 155(2) of the Islamic Financial Services Act 2013 (IFSA); and
(c) Sections 41(1) and 116(1) of the Development Financial Institutions Act 2002 (DFIA).

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

4 Effective date

4.1 This policy document comes into effect on 1 January 2020.

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 or DFIA, 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;

"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 or payment 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, in particular, the account, of any customer or counterparty of a financial institution in whatever form;

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

"cyber risk" refers to threats or vulnerabilities emanating from the connectivity of internal technology infrastructure to external networks or the Internet;

"digital services" refers to the provision of payment, 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;

"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 development financial institution under the DFIA;
(c) an eligible issuer of e-money as defined in the policy document on Interoperable Credit Transfer Framework[1]; and
(d) an operator of a designated payment system;

"large financial institution" refers to-
(a) a financial institution with one or more business lines that are significant in terms of market share in the relevant industry; or
(b) a financial institution with a large network of offices within or outside Malaysia through operations of branches and subsidiaries;

"material technology projects" refers to projects which involve critical systems, the delivery of essential services to customers or counterparties, or compliance with regulatory requirements;

"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;

"public cloud" refers to a fully virtualised environment in which a service provider makes resources such as platforms, applications or storage available to the public over the Internet via a logically separated multi-tenant architecture;

"production data centre" refers to any facility which hosts active critical production application systems irrespective of location;

"recovery data centre" refers to a facility that a financial institution plans to activate to recover and restore its IT applications and operations upon failure of its production data centre irrespective of location;

"senior management" refers to the Chief Executive Officer (CEO) and senior officers;

"third party service provider" refers to an internal group affiliate or external entity providing technology-related functions or services that involve 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.

[1] For ease of reference, an "eligible issuer of e-money" 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 Interoperable Credit Transfer Framework.

6 Related legal instruments and policy documents

6.1 This policy document must be read together with any relevant legal instruments, policy documents and guidelines issued by the Bank, in particular—

(a) Policy Document on Risk Governance;
(b) Policy Document on Compliance;
(c) Policy Document on Outsourcing;
(d) Policy Document on Operational Risk;
(e) Policy Document on Operational Risk Reporting Requirement – Operational Risk Integrated Online Network (ORION);
(f) Policy Document on Introduction of New Products;
(g) Policy Document on Interoperable Credit Transfer Framework;
(h) Guidelines on Business Continuity Management (Revised);
(i) Provisions under paragraphs 21, 22 and 26 of the Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions;
(j) Provisions under paragraphs 28 and 29 of the Guidelines on Internet Insurance (Consolidated);
(k) Guidelines on Data Management and MIS Framework;
(l) Guidelines on Data Management and MIS Framework for Development Financial Institutions; and
(m) Paragraphs 3 and 5 of the Circular on Internet Takaful[2].

7 Policy documents and circulars superseded

7.1 This policy document supersedes the following circulars, guidelines and policy documents:

(a) Guidelines on Management of IT Environment (GPIS 1) issued in May 2004;
(b) Preparedness against Distributed Denial of Service Attack issued on 17 October 2011;
(c) Managing Inherent Risk of Internet Banking Kiosks issued on 5 December 2011;
(d) Circular on Managing Risks of Malware Attacks on Automated Teller Machine (ATM) issued on 3 October 2014;
(e) Managing Cyber Risk Circular issued on 31 July 2015;
(f) Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions, except for the provisions under paragraphs 21, 22 and 26;
(g) Guidelines on Internet Insurance (Consolidated), except for the provisions under paragraphs 28 and 29;
(h) Circular on Internet Takaful, except for paragraphs 3 and 5;
(i) Letter to CEO dated 31 October 2017 entitled “Immediate Measures for Managing identification of Counterfeit Malaysian Currency Notes at Deposit-Accepting Self Service Terminals (SST)”;

[2] For the avoidance of doubt, only the requirements not superseded in this policy document are applicable.

(j) Letter to CEO dated 7 November 2017 entitled “Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions (“Guidelines”) – Specification Pursuant to the Financial Services Act 2013 (“FSA”), Islamic Financial Services Act 2013 (“IFSA”) and Development Financial Institutions Act 2002 (“DFIA”)”;
(k) Letter to CEO dated 10 November 2017 entitled “Storage and Transportation of Sensitive Data in Removable Media”;
(l) Letter to CEO dated 17 May 2018 entitled “Guidelines on Internet Insurance (Consolidated) (“Guidelines”) and Circular on Internet Takaful (“the Circular’) – Specification Pursuant to the Financial Services Act 2013 (“FSA”) and Islamic Financial Services Act 2013 (“IFSA”)”;
(m) Letter to CEO dated 11 December 2018 entitled “Leveraging on cloud services and upliftment of mobile banking condition”; and
(n) Letter to CEO dated 18 November 2019 entitled "Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions, Guidelines on Internet Insurance (Consolidated), Circular on Internet Takaful - Specification Pursuant to the Financial Services Act 2013 ("FSA"), Islamic Financial Services Act 2013 ("IFSA") and the Development Financial Institutions Act 2002 ("DFIA")”.

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 approve the corresponding risk tolerances for technology-related events and ensure key performance indicators and forward-looking risk indicators are in place to monitor the financial institution's technology risk against its approved risk tolerance. The board must ensure senior management provides regular updates on the status of these indicators together with sufficiently detailed information on key technology risks and critical technology operations to facilitate strategic decision-making.

S 8.2 The board must ensure and oversee the adequacy of the financial institution's IT and cybersecurity strategic plans covering a period of no less than three years. These plans shall address the financial institution's requirements on infrastructure, control measures to mitigate IT and cyber risk and financial and non-financial resources, which are commensurate with the complexity of the financial institution's operations and changes in the risk profile as well as the business environment. These plans shall be periodically reviewed, at least once every three years.

S 8.3 The board shall be responsible to 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 financial institution to ensure the continuity of operations and delivery of financial services. The TRMF is a framework to safeguard the financial institution's information infrastructure, systems and data, whilst the CRF is a framework for ensuring the financial institution's cyber resilience. The board must ensure that the financial institution's TRMF and CRF remain relevant on an ongoing basis. The board must also periodically review and affirm the TRMF and CRF, at least once every three years to guide the financial institution's management of technology risks.

S 8.4 The board must designate a board-level committee[3] which shall be responsible for supporting the board in providing oversight over technology-related matters. Among other things, the committee shall review the technology-related frameworks including the requirements spelt out in paragraphs 8.1 through 8.3, for the board's approval, and ensure that risk assessments undertaken in relation to material technology applications submitted to the Bank are robust and comprehensive.

[3] 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.

G 8.5 To promote effective technology discussions at the board level, the composition of the board and the designated board-level committee should include at least a member with technology experience and competencies.

S 8.6 Given the rapidly evolving cyber threat landscape, the board shall allocate sufficient time to discuss cyber risks and related issues, including the strategic and reputational risks associated with a cyber-incident. This shall be supported by input from external experts as appropriate. The board must also ensure its continuous engagement in cybersecurity preparedness, education and training.

S 8.7 The board audit committee (BAC) is responsible for ensuring the effectiveness of the internal technology audit function. This includes 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 must also ensure effective oversight over the prompt closure of corrective actions to address technology control gaps.

Responsibilities of the senior management

S 8.8 A financial institution's senior management must translate the board-approved TRMF and CRF into specific policies and procedures that are consistent with the approved risk appetite and risk tolerance and supported by effective reporting and escalation procedures.

S 8.9 The senior management must establish a cross-functional committee to provide guidance on the financial institution's technology plans and operations. Members of the committee must include senior management from both technology functions and 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[4]; and
(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.

S 8.10 Senior management must ensure the adequate allocation of resources to maintain robust technology systems and appropriately skilled and competent staff to support the effective management of technology risk.

S 8.11 For large financial institutions, senior management must embed appropriate oversight arrangements within the technology function to support the enterprise-wide oversight of technology risk. These arrangements must provide for designated staff responsible for the identification, assessment and

[4] 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 and utilisation of the technology budget.

mitigation of technology risks who do not engage in day-to-day technology operations.

S 8.12 For the purpose of paragraph 8.11 and all other requirements applicable to large financial institutions under this policy document, each financial institution shall conduct a self-assessment on whether it is a large financial institution in accordance with the definition in paragraph 5.2. The self-assessment shall take into account–

(a) the complexity of the financial institution's operations, having particular regard to the interconnectedness of its operations with other financial institutions, customers and counterparties that are driven by technology;
(b) the number and size of the financial institution's significant business lines together with its market share[5] (e.g. in terms of assets, liabilities, revenue and premiums);
(c) the number of subsidiaries, branches and agents; and
(d) other business considerations that could give rise to technology risk.

S 8.13 Notwithstanding the self-assessment in paragraph 8.12, the Bank may designate a financial institution as a large financial institution and such financial institutions shall comply with all requirements in this policy document applicable to a large financial institution.

9 Technology Risk Management

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;
(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; and
(g) continuous monitoring to timely detect and address any material risks.

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

[5] Size is an indicator of the potential systemic impact that any failure or breach of the financial institution's IT systems may have on the broader financial system. When determining the significance of its size, the financial institution shall consider the extent to which the broader market segment may be unable to access relevant financial services in the event of a disruption to its systems. It should also consider the extent to which the operations of other institutions may be disrupted due to a reliance on services provided by the financial institution that may not be immediately substitutable.

(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[6], where necessary.

S 9.4 A financial institution must designate a Chief Information Security Officer (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[7]. The CISO shall—
(a) be independent from day-to-day technology operations;
(b) keep apprised of current and emerging technology risks which could potentially affect the financial institution's risk profile; and
(c) be appropriately certified.

S 9.5 The CISO is responsible for ensuring 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.

10 Technology Operations Management

Technology Project Management

S 10.1 A financial institution must establish appropriate governance requirements commensurate with the risk and complexity[8] 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

[6] Relevant third party assessments may include the Data Centre Risk Assessment (DCRA), Network Resilience and Risk Assessment (NRA) and independent assurance for introduction of new or enhanced digital services.
[7] 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. 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.
[8] For example, large-scale integration projects or those involving critical systems should 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.

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.

System Development and Acquisition

G 10.4 A financial institution should establish an enterprise architecture framework (EAF) that provides a holistic view of technology throughout the financial institution. The EAF is an overall technical design and high-level plan that describes the financial institution’s technology infrastructure, systems’ inter-connectivity and security controls. The EAF facilitates the conceptual design and maintenance of the network infrastructure, related technology controls and policies, and serves as a foundation on which financial institutions plan and structure system development and acquisition strategies to meet business goals.

S 10.5 A financial institution must establish clear risk management policies and practices for the key phases of the system development life cycle (SDLC) encompassing system design, development, testing, deployment, change management, maintenance and decommissioning. Such policies and practices must also embed security and relevant enterprise architecture considerations into the SDLC to ensure confidentiality, integrity and availability

of data[9]. The policies and practices must be reviewed at least once every three years to ensure that they remain relevant to the financial institution's environment.

G 10.6 A financial institution is encouraged to deploy automated tools for software development, testing, software deployment, change management, code scanning and software version control to support more secure systems development.

S 10.7 A financial institution shall consider the need for diversity[10] in technology to enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.

S 10.8 A financial institution must establish a sound methodology for 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 should include unit testing, integration testing, user acceptance testing, application security testing, stress and regression testing, and 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 was developed in line with recognised coding practices prior to introducing any system changes.

S 10.11 In relation to critical systems that are developed and maintained by vendors, a financial institution must ensure the source code continues to be readily accessible and secured from unauthorised access.

S 10.12 A financial institution shall physically segregate the production environment from the development and testing environment for critical 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 10.13 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 unsuccessful implementation of material changes to minimise any business disruption.

S 10.14 Where a financial institution's IT systems are managed by third party service providers, the financial institution shall ensure, including through contractual obligations, that the third party service providers provide sufficient notice to the

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

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

financial institution before any changes are undertaken that may impact the IT systems.

S 10.15 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.

Cryptography

S 10.16 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 every three years, of existing cryptographic standards and algorithms in critical systems, external linked or transactional customer-facing applications to prevent exploitation of weakened algorithms or protocols; and

(d) 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.

S 10.17 A financial institution shall ensure clear senior-level roles and responsibilities are assigned for the effective implementation of the cryptographic policy.

S 10.18 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. Where a 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. Where this involves a reliance on third party assessments[11], the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A 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.

[11] 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.

S 10.19 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) or trusted execution environment (TEE).

S 10.20 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.

Data Centre Resilience

Data Centre Infrastructure

S 10.21 A financial institution must specify the resilience and availability objectives of its data centres which are aligned with its business needs. The network infrastructure must be designed to be resilient, secure and scalable. Potential data centre failures or disruptions must not significantly degrade the delivery of its financial services or impede its internal operations.

S 10.22 A financial institution must ensure production data centres are concurrently maintainable. This includes ensuring that production data centres have redundant capacity components and distribution paths serving the computer equipment.

S 10.23 In addition to the requirement in paragraph 10.22, large financial institutions are also required to ensure recovery data centres are concurrently maintainable.

S 10.24 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 (SPOF) 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 10.25 A financial institution is required to appoint a technically competent external service provider to carry out a production data centre resilience and risk assessment (DCRA) and set proportionate controls aligned with the financial institution's risk appetite. 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 whenever 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 10.22 to 10.24 have been adhered to. For data centres managed by third party service providers, a financial institution may 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 expectations in this paragraph for conducting the DCRA. The designated board-level committee must deliberate the outcome of the assessment.

Data Centre Operations

S 10.26 A financial institution must ensure its capacity needs are well-planned and managed with due regard to business growth plans. This includes ensuring adequate system storage, central processing unit (CPU) power, memory and network bandwidth. A financial institution shall involve both the technology stakeholders and the relevant business stakeholders within the financial institution in its development and implementation of capacity management plans.

S 10.27 A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services[12]. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.

S 10.28 A financial institution must segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity[13]. In the case where vendors' or programmers' access to the production environment is necessary, these activities must be properly authorised and monitored.

S 10.29 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 10.30 A financial institution is required to undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that

[12] For example, batch runs and backup processes for the financial institution's application systems and infrastructure.

[13] For example, system development activities must be segregated from data centre operations.

existing controls are adequate in protecting sensitive data at all times. A financial institution must also maintain a sufficient number of backup copies of 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. Backup media must be stored in an environmentally secure and access-controlled backup site.

G 10.31 In regard to paragraph 10.30, a financial institution should also adopt the controls as specified in Appendix 1 or their equivalent to secure the storage and transportation of sensitive data in removable media.

S 10.32 Where there is a reasonable expectation for immediate delivery of service to customers or dealings with counterparties, a financial institution must ensure that the relevant critical 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.

Network Resilience

S 10.33 A financial institution must design a reliable, scalable and secure enterprise network that is able to support its business activities, including future growth plans.

S 10.34 A financial institution must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats[14].

S 10.35 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 10.36 A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.

S 10.37 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 10.38 A financial institution must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years.

[14] Measures implemented may include component redundancy, service diversity and alternate network paths.

S 10.39 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.

S 10.40 A financial institution is required to 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. 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 10.33 to 10.39. The designated board-level committee must deliberate the outcome of the assessment.

Third Party Service Provider Management

S 10.41 The board and senior management of the financial institution must exercise effective oversight and address associated risks when engaging third party service providers[15] for critical technology functions and systems. Engagement of third party service providers, including engagements for independent assessments, does not in any way reduce or eliminate the principal accountabilities and responsibilities of financial institutions for the security and reliability of technology functions and systems.

S 10.42 A financial institution must conduct proper due diligence on the third party service provider's competency, system infrastructure and financial viability as relevant prior to engaging its services. In addition, an assessment shall be made of the third party service provider's capabilities in managing the following specific risks–

(a) data leakage such as unauthorised disclosure of customer and counterparty information;
(b) service disruption including capacity performance;
(c) processing errors;
(d) physical security breaches;
(e) cyber threats;
(f) over-reliance on key personnel;
(g) mishandling of confidential information pertaining to the financial institution or its customers in the course of transmission, processing or storage of such information; and
(h) concentration risk.

S 10.43 A financial institution must establish service-level agreements (SLA) when engaging third party service providers. 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

[15] Financial institutions 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.

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 service provider to provide sufficient prior notice to financial institutions of any sub-contracting which is substantial;

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

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

(e) critical system availability; and

(f) arrangements to secure business continuity in the event of exit or termination of the service provider.

S 10.44 A financial institution must ensure its ability to regularly review the SLA with its third party service providers to take into account the latest security and technological developments in relation to the services provided.

S 10.45 A financial institution must ensure its third party service providers comply with all relevant regulatory requirements prescribed in this policy document[16].

S 10.46 A financial institution must ensure data residing in third party service providers are recoverable in a timely manner. The financial institution shall ensure clearly defined arrangements with the third party service provider are in place to facilitate the financial institution's immediate notification and timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident.

S 10.47 A financial institution must ensure the storage of its data is at least logically segregated from the other clients of the third party service provider. There shall be proper controls over and periodic review of the access provided to authorised users.

S 10.48 A financial institution must ensure any critical system hosted by third party service providers have strong recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by the third party service provider.

Cloud Services

S 10.49 A financial institution must fully understand the inherent risk of adopting cloud services. In this regard, a financial institution is required to 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;

[16] This includes specific requirements for system development and acquisition, data centre operations, network resilience, technology security and cybersecurity, wherever applicable.

(b) migration of existing systems to cloud infrastructure;
(c) location of cloud infrastructure;
(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 service provider; and
(j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.

S 10.50 A financial institution must separately identify critical and non-critical systems prior to using any cloud services, guided by the definition of "critical system" in paragraph 5.2. A financial institution must notify the Bank of its intention to use cloud services for non-critical systems. The risk assessment as outlined in paragraph 10.49 must be documented and made available for the Bank's review as and when requested by the Bank.

S 10.51 A financial institution is required to consult the Bank prior to the use of public cloud for critical systems. The financial institution is expected to demonstrate that specific risks associated with the use of cloud services for critical systems have been adequately considered and addressed. The risk assessment shall address the risks outlined in paragraph 10.49 as well as the following areas:

(a) the adequacy of the over-arching cloud adoption strategy of the financial institution including:
    (i) board oversight over cloud strategy and cloud operational management;
    (ii) senior management roles and responsibilities on cloud management;
    (iii) conduct of day-to-day operational management functions;
    (iv) management and oversight by the financial institution of cloud service providers;
    (v) quality of risk management and internal control functions; and
    (vi) strength of in-house competency and experience;

(b) the availability of independent, internationally recognised certifications of the cloud service providers, at a minimum, in the following areas:
    (i) information security management framework, including cryptographic modules such as used for encryption and decryption of user data; and
    (ii) cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in use, in storage and in transit; and

(c) the degree to which the selected cloud configuration adequately addresses the following attributes:
    (i) geographical redundancy;
    (ii) high availability;

(iii) scalability;
(iv) portability;
(v) interoperability; and
(vi) strong recovery and resumption capability including appropriate alternate Internet path to protect against potential Internet faults.

S 10.52 A financial institution shall consider the need for a third party pre-implementation review on cloud implementation that also covers the areas set out in paragraph 10.51.

S 10.53 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 10.54 A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems.

G 10.55 In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy:
(a) adopt a “deny all” access control policy for users by default unless explicitly authorised;
(b) employ “least privilege” access rights or 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 rights which restrict access to a specific period including access rights granted to service providers;
(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; and
(iii) network operation and network security;
(e) employ dual control functions which require two or more persons to execute an activity;
(f) adopt stronger authentication for critical activities including for remote access;
(g) limit and control the use of the same user ID for multiple concurrent sessions;
(h) limit and control the sharing of user ID and passwords across multiple users; and

(i) control the use of generic user ID naming conventions in favour of more personally identifiable IDs.

S 10.56 A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).

S 10.57 A financial institution shall periodically review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There must be appropriate controls in place to check the strength of the passwords created.

G 10.58 Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial institutions are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents.

G 10.59 A financial institution is encouraged to adopt dedicated user domains for selected critical functions, separate from the broader enterprise-wide user authentication system.

S 10.60 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 10.61 A financial institution must ensure—

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

(b) 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.

S 10.62 In fulfilling the requirement under paragraph 10.61, large financial institutions are required to—

(a) deploy an identity access management system to effectively manage and monitor user access to enterprise-wide systems; and

(b) deploy automated audit tools to flag any anomalies.

Patch and End-of-Life System Management

S 10.63 A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions:

(a) to continuously monitor and implement latest patch releases in a timely manner; and
(b) identify critical technology systems that are approaching EOL for further remedial action.

S 10.64 A large financial institution must establish dedicated resources to perform the functions under paragraph 10.63.

S 10.65 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) conduct of compatibility testing for critical patches;
(c) specification of turnaround time for deploying patches according to the severity of the patches; and
(d) adherence to the workflow for end-to-end patch deployment processes including approval, monitoring and tracking of activities.

Security of Digital Services

S 10.66 A financial institution must implement robust technology security controls in providing digital services which assure the following:
(a) confidentiality and integrity of customer and counterparty information and transactions;
(b) reliability of services delivered via channels and devices with minimum disruption to services;
(c) proper authentication of users or devices and authorisation of transactions;
(d) sufficient audit trail and monitoring of anomalous transactions;
(e) ability to identify and revert to the recovery point prior to incident or service disruption; and
(f) strong physical control and logical control measures.

S 10.67 A financial institution must implement controls to authenticate and monitor all financial transactions. These controls, at a minimum, must be effective in mitigating man-in-the-middle attacks, transaction fraud, phishing and compromise of application systems and information.

S 10.68 A financial institution must implement additional controls to authenticate devices and users, authorise transactions and support non-repudiation and accountability for high-risk transactions or transactions above RM10,000. These measures must include, at a minimum, the following:
(a) ensure transactions are performed over secured channels such as the latest version of Transport Layer Security (TLS);
(b) both client and host application systems must encrypt all confidential information prior to transmission over the network;
(c) adopt MFA for transactions;
(d) if OTP is used as a second factor, it must be dynamic and time-bound;
(e) request users to verify details of the transaction prior to execution;
(f) ensure secure user and session handling management;

(g) be able to capture the location of origin and destination of each transaction;
(h) 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); and
(i) provide timely notification to customers that is sufficiently descriptive of the nature of the transaction.

S 10.69 A financial institution must ensure the MFA solution used to authenticate financial transactions are adequately secure, which includes the following:
(a) binding of the MFA solution to the customer's account;
(b) activation of MFA must be subject to verification by the financial institution; and
(c) timely notification to customers of any activation of and changes to the MFA solution via the customers' verified communication channel.

G 10.70 A financial institution should deploy MFA technology and channels that are more secure than unencrypted short messaging service (SMS).

S 10.71 A financial institution shall deploy MFA solutions with stronger security controls for open third party fund transfer and open payment transactions with a value of RM10,000 and above.

S 10.72 Such stronger MFA solutions shall adhere to the following requirements:
(a) payer/sender must be made aware and prompted to confirm details of the identified beneficiary and amount of the transaction;
(b) authentication code must be initiated and generated locally by the payer/sender using MFA;
(c) authentication code generated by payer/sender must be specific to the confirmed identified beneficiary and amount;
(d) secure underlying technology must be established to ensure the authentication code accepted by the financial institution corresponds to the confirmed transaction details; and
(e) notification must be provided to the payer/sender of the transaction.

S 10.73 Where a financial institution deploys OTP as part of its stronger MFA solutions, the following features must be implemented:
(a) binding of the transaction details to the OTP generated by the device (e.g. beneficiary account number, amount of transaction);
(b) generation of the OTP from the customer's device and not from the bank's server; and
(c) requiring the customer to physically enter the generated OTP into the application.

S 10.74 For financial transactions below RM10,000, a financial institution may decide on proportionate controls and authentication methods for transactions assessed by the financial institution to be of low risk. In undertaking the assessment, the financial institution must establish a set of criteria or factors that reflect the nature, size and characteristics of a financial transaction. Such criteria or factors must be consistent with the financial institution's risk appetite

and tolerance. The financial institution must periodically review the risk assessment criteria to ensure its continued relevance, having regard to the latest developments in cybersecurity risks and authentication technologies as well as fraud trends and incidents.

S 10.75 Where a financial institution decides not to adopt MFA for financial transactions that are assessed to be of low risk, the financial institution must nevertheless implement adequate safeguards for such transactions which shall include at a minimum the following measures:

(a) set appropriate limits on a per-transaction basis, and on a cumulative basis;
(b) provide a convenient means for customers to reduce the limits described in paragraph (a) or to opt for MFA;
(c) provide a convenient means for its customers to temporarily suspend their account in the event of suspected fraud; and
(d) provide its customers with adequate notice of the safeguards set out in sub-paragraphs (a) to (c).

S 10.76 A financial institution must ensure sufficient and relevant digital service logs are retained for investigations and forensic purposes for at least three years.

S 10.77 A financial institution must ensure that critical online payments and banking[17] services have high availability with reasonable response time to customer actions.

S 10.78 A financial institution must ensure that the use of more advanced technology to authenticate and deliver digital services such as biometrics, tokenisation and contactless communication[18] comply with internationally recognised standards where available. The technology must be resilient against cyber threats[19] including malware, phishing or data leakage.

S 10.79 A financial institution must undertake a comprehensive risk assessment of the advanced technologies and the algorithms deployed in its digital services. Algorithms must be regularly reviewed and validated to ensure they remain appropriate and accurate. Where third party software is used, a financial institution may rely on relevant independent reports provided such reliance is consistent with the financial institution's risk appetite and tolerance, and the nature of digital services provided by the financial institution which leverage on the technologies and algorithms.

S 10.80 A financial institution must ensure authentication processes using biometric technology are secure, highly resistant to spoofing and have a minimal false acceptance rate to ensure confidentiality, integrity and non-repudiation of transactions.

[17] For example, Internet and mobile banking services.
[18] Such as Quick Response (QR) code, Bar Code, Near Field Communication (NFC), Radio Frequency Identification (RFID), Wearables.
[19] For example, in respect of QR payments, financial institutions shall implement safeguards within its respective mobile applications to detect and mitigate risks relating to QR code that may contain malware or links to phishing websites.

S 10.81 A financial institution must perform continuous surveillance to assess the vulnerability of the operating system and the relevant technology platform used for its digital delivery channels to security breaches and implement appropriate corresponding safeguards. At a minimum, a financial institution must implement sufficient logical and physical safeguards for the following channels:

(a) self-service terminal (SST);
(b) non-cash SST;
(c) Internet banking; and
(d) mobile application and devices.

In view of the evolving threat landscape, these safeguards must be continuously reviewed and updated to protect against fraud and to secure the confidentiality and integrity of customer and counterparty information and transactions.

G 10.82 In fulfilling paragraph 10.81, a financial institution should adopt the controls specified in the following Appendices for the respective digital delivery channel:

(a) Appendix 2: Control Measures on Self-Service Terminals (SST);
(b) Appendix 3: Control Measures on Internet Banking; and
(c) Appendix 4: Control Measures on Mobile Application and Devices.

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 the institution's 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-premise 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 and countermeasures including measures to contain reputational damage that can undermine confidence in the financial institution;
(d) layered (defense-in-depth) security controls to protect its data, infrastructure and assets against evolving 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; and
(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.

S 11.4 In addition to the requirements in paragraph 11.3, a large financial institution is required to—
(a) implement a centralised automated tracking system to manage its technology asset inventory; and
(b) establish a dedicated in-house cyber risk management function to manage cyber risks or emerging cyber threats. The cyber risk management function shall be responsible for the following:
(i) perform detailed analysis on cyber threats, provide risk assessments on potential cyber-attacks and ensure timely review and escalation of all high-risk cyber threats to senior management and the board; and
(ii) proactively identify potential vulnerabilities including those arising from infrastructure hosted with third party service providers through the simulation of sophisticated “Red Team” attacks on its current security controls.

Cybersecurity Operations

S 11.5 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.

G 11.6 Where relevant, a financial institution should adopt the control measures on cybersecurity as specified in Appendix 5 to enhance its resilience to cyber-attacks.

S 11.7 A financial institution must deploy effective tools to support the continuous and proactive monitoring and timely detection of anomalous activities in its

technology infrastructure. The scope of monitoring must cover all critical systems including the supporting infrastructure.

S 11.8 A financial institution must ensure that its cybersecurity operations continuously prevent and detect any potential compromise of its security controls or weakening of its security posture. For large financial institutions, this must include performing a quarterly vulnerability assessment of external and internal network components that support all critical systems.

S 11.9 A financial institution must conduct annual intelligence-led penetration tests on its internal and external network infrastructure as well as critical systems including web, mobile and all external-facing applications. The penetration testing 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.

S 11.10 In addition to the requirement in paragraph 11.9, a large financial institution must undertake independent compromise assessments on the technology infrastructure of its critical systems at least annually and ensure the results of such assessments are escalated to senior management and the board in a timely manner.

S 11.11 A financial institution must establish standard operating procedures (SOP) for vulnerability assessment and penetration testing (VAPT) activities. The SOP must outline the relevant control measures including ensuring the external penetration testers are accompanied on-premises at all times, validating the event logs and ensuring data purging.

S 11.12 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.

Distributed Denial of Service (DDoS)

S 11.13 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 DDoS attacks (including 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;

(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 mechanisms to mitigate against Domain Name Server (DNS) based layer attacks.

Data Loss Prevention (DLP)

S 11.14 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.

S 11.15 A financial institution must design internal control procedures and implement appropriate technology in all applications and access points to enforce 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.

S 11.16 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.

Security Operations Centre (SOC)

S 11.17 A financial institution must ensure its SOC, whether managed in-house or by third party service providers, 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.

S 11.18 The SOC must be able to perform the following functions:

(a) 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; and
(f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, and monitoring indicators of compromise (IOC). 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.

S 11.19 A financial institution must ensure that the SOC provides a regular 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).

For large financial institutions, such reports shall be provided on a monthly basis.

S 11.20 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.

S 11.21 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.

Cyber Response and Recovery

S 11.22 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 11.23 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 the extent of damage and preserving sufficient evidence for forensics purposes;

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

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

S 11.24 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. A key contact person or an alternate must be appointed to liaise with the Bank during an incident.

S 11.25 A financial institution must conduct an annual cyber drill exercise to test the effectiveness of its CIRP, 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 test scenarios must include scenarios designed to test:
(a) the effectiveness of escalation, 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 11.26 A financial institution must immediately notify the Bank of any cyber-incidents affecting the institution. Upon completion of the investigation, the financial institution is also required to submit a report on the incident through ORION[20].

G 11.27 Financial institutions are strongly encouraged to collaborate and cooperate closely with relevant stakeholders and competent authorities in combating cyber threats and sharing threat intelligence and mitigation measures.

12 Technology Audit

S 12.1 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 12.2 The internal audit function must be adequately resourced with relevant technology audit competencies and sound knowledge of the financial institution's technology processes and operations.

S 12.3 A financial institution must ensure its internal technology audit staff are professionally certified and adequately conversant with the developing sophistication of the financial institution's technology systems and delivery channels.

S 12.4 In addition to paragraph 12.2, a large financial institution must establish a dedicated internal technology audit function that has specialised technology audit competencies to undertake technology audits.

[20] Operational Risk Integrated Online Network

S 12.5 A financial institution must establish a technology audit plan that provides appropriate 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.

G 12.6 The internal audit function (in the case of paragraph 12.2) and the dedicated internal technology audit function (in the case of paragraph 12.4) may be enlisted to provide advice on compliance with and adequacy of control processes during the planning and development phases of new major products, systems or technology operations. In such cases, the technology auditors participating in this capacity should carefully consider whether such an advisory or consulting role would materially impair their independence or objectivity in performing post-implementation reviews of the products, systems and operations concerned.

13 Internal Awareness and Training

S 13.1 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 programmes. This cybersecurity awareness education must be conducted at least annually by the financial institution and must reflect the current cyber threat landscape.

S 13.2 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 to effectively perform their roles and responsibilities.

S 13.3 In fulfilling the requirements under paragraph 13.2, a large financial institution shall ensure the staff working on day-to-day IT operations such as IT security, project management and cloud operations are also suitably certified.

S 13.4 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

14 Notification for Technology-Related Applications

S 14.1 A financial institution must notify the Bank in accordance with the requirements in paragraphs 14.2 to 14.7 prior to conducting e-banking, Internet insurance and Internet takaful services, including introducing new technology relating to e-banking, Internet insurance and Internet takaful[21].

S 14.2 A financial institution offering e-banking, Internet insurance and Internet takaful services for the first time must submit the following information in the notification to the Bank:

(a) 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 for e-banking, Internet insurance and Internet takaful services;
(d) client charter on e-banking, Internet insurance and Internet takaful services;
(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 14.3 In introducing any enhancement to existing e-banking, Internet insurance and Internet takaful services, the financial institution is required to follow the notification process based on whether the enhancement is explicitly listed in Appendix 6 (Positive List for Enhancement to Electronic Banking, Internet Insurance and Internet Takaful Services). The list may be updated as and when there are changes to the risk profile and risk management of the technology landscape.

S 14.4 For any enhancements listed in Appendix 6, the financial institution must submit the notification together with the following information:

(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 14.5 For the introduction of new services, and any enhancements to existing services not listed in Appendix 6, the 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

[21] For the purpose of this Part,–
"**e-banking**" means the provision of banking products and services through electronic channels. E-banking includes banking via the Internet, phone, automated teller machines (ATM), and any other electronic channel.
"**Internet insurance**" means the use of the Internet as a channel to transact insurance business with customers or as a platform for transmission of customers' information; and
"**Internet takaful**" means the use of the Internet as a channel to transact takaful business with customers or as a platform for transmission of customers' information.

controls associated with the e-banking, Internet insurance and Internet takaful services or any material enhancement to the existing e-banking, Internet insurance and Internet takaful services. The format of the assurance shall be as set out in Appendix 7; and

(b) provide a confirmation by the CISO, senior management officer or the chairman of the board or designated board-level committee stipulated in paragraph 8.4 of the financial institution's readiness to provide e-banking, Internet insurance and Internet takaful services or implement any material enhancement to the e-banking, Internet insurance and Internet takaful services. The format of the confirmation shall be as set out in Appendix 8.

S 14.6 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, Appendix 9.

G 14.7 For any enhancements that do not materially alter the prior assessments and representations made by a financial institution to the Bank, a notification under paragraph 14.4 and Appendix 6 is not required. However, a financial institution should have the relevant information readily available upon request by the Bank to facilitate the ongoing supervisory process.

G 14.8 A financial institution may offer the services or implement any enhancement to the services immediately upon submission of the notification under paragraph 14.1 and compliance with the requirements in paragraphs 14.2 to 14.6.

15 Assessment and Gap Analysis

S 15.1 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 particularly for gaps that extend beyond the effective date of this policy document. The gap analysis and action plan must be submitted to the Bank no later than 18 October 2019.

S 15.2 For the purpose of paragraph 8.12, a financial institution shall submit together with the gap analysis and action plan its self-assessment on whether it is a large financial institution.

S 15.3 The self-assessment, gap analysis and action plan in paragraphs 15.1 and 15.2 must be submitted to Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan, Jabatan Penyeliaan Insurans dan Takaful or Jabatan Pemantauan Pembayaran, as the case may be.

Appendix 1 Storage and Transportation of Sensitive Data in Removable Media

Financial institutions should 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. Should there be a need to transport the removable media to a different physical location, financial institutions must—
   (a) strengthen the chain of custody process 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 should 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 tries;
   (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. Ensuring Cash SST operating system is running on a secure version operating system with continued developer or vendor support for security patches to fix any operating system security and vulnerabilities;
4. Deploying Anti-virus (AV) solution for Cash SST and ensure timely update of signatures. Ensure virus scanning on all Cash SSTs is performed periodically;
5. Implementing a centralised management system to monitor and alert any unauthorised activities on Cash SST such as unauthorised shutting-down of OS or deactivation of the white-listing programme;
6. 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;
7. 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;
8. Securing physically the Cash SST PC Core by enclosing the CPU in a locked case;
9. Enforcing firewall and Intrusion Prevention System (IPS) at the financial institution’s network to filter communication between the host server and the Cash SST;
10. Enforcing pairing authentication for key Cash SST components, particularly between cash dispenser and Cash SST controller;
11. Enforcing Basic Input Output System (BIOS) lock-down which includes:

(a) enabling unique password protection for accessing BIOS. The password should 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;

12. Ensuring proper configuration and hardening of the OS 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;

13. Enforcing secure system parameter setting, which includes:

(a) changing defaults password 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;

14. Performing scanning and removing any known malware such as Backdoor.Padpin and Backdoor.Ploutus;

15. Enforcing and monitor 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;

16. Enforcing strict control procedures over installation and maintenance of Cash SST OS 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

17. 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 and cheque deposit machines that provide non-cash transactions such as cheque deposits, balance enquiries, fund transfers, utilities bill payments and insurance quotations.

Financial institutions should 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 central processing unit (CPU) at all times;
2. Deploying closed-circuit television to monitor the usage of self-service terminals;
3. Ensuring adequate control over network security of the self-service terminals to ensure that the kiosks are secured and segregated from the internal network;
4. 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;
5. Disabling browser scripting, pop-ups, ActiveX, Windows shortcut;
6. Concealing Start Bar or Tray Menu;
7. Enabling cache auto-deletion;
8. Disabling key combinations and right-click mouse functions; and
9. Restricting use of Internet browser i.e. only to be used to access the financial institution's internet website.

Appendix 3 Control Measures on Internet Banking

1. A financial institution should ensure the adequacy of security controls implemented for Internet banking, which include:

   (a) Ensure Internet banking only runs on secured versions of web browsers that have continued developer support for security patches to fix any vulnerabilities;

   (b) 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 should require the customer to acknowledge that the image or word is correct before the password box is displayed to the customer;

   (c) Assign a customer to MFA solution binding to a single device;

   (d) Require MFA when registering an account as a "favourite" beneficiary. A financial institution must also require MFA, for the first funds transfer to the favourite beneficiary;

   (e) For new customers, the default transfer limit shall be set at a conservatively low level (such as RM5,000 per day). However, customers should be provided with the option to change the limit via secure channels (e.g. online with MFA or at branches); and

   (f) Deploy an automated fraud detection system which has the capability to conduct heuristic behavioural analysis.

Appendix 4 Control Measures on Mobile Application and Devices

1. A financial institution should ensure digital payment, banking and insurance services involving sensitive customer and counterparty information offered via mobile devices are adequately secured. This includes the following:
   (a) ensure mobile applications run only on the supported version of operating systems and enforce the application to only operate on a secure version of operating systems which have not been compromised, jailbroken or rooted i.e. the security patches are up-to-date;
   (b) design the mobile application to operate in a secure and tamper-proof environment within the mobile devices. The mobile application shall be prohibited 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 shall be centralised at the host;
   (c) undertake proper due diligence processes to ensure the application distribution platforms used to distribute the mobile application are reputable;
   (d) ensure proper controls are in place to access, maintain and upload the mobile application on application distribution platforms;
   (e) activation of the mobile application must be subject to authentication by the financial institution;
   (f) ensure secure provisioning process of mobile application in the customer's device is in place by binding the mobile application to the customer's profile such as device ID and account number; and
   (g) monitor the application distribution platforms to identify and address the distribution of fake applications in a timely manner.

2. In addition to the guidance in paragraph 1, a financial institution should 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) establish safeguards that ensure the security of customer and counterparty information (e.g. Primary Account Numbers (PAN), Card Verification Value Numbers (CVV), expiry dates and Personal Identification Numbers (PIN) of payment cards), including to mitigate risks of identity theft and fraud[22];
   (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 businesses in mobile devices to 30 days.

[22] 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

1. Conduct periodic review on the configuration and rules settings for all security devices. Use automated tools to review and monitor changes to configuration and rules settings.
2. Update checklists on the latest security hardening of operating systems.
3. Update security standards and protocols for web services encryption regularly. Disable support of weak ciphers and protocol in web-facing applications.
4. Ensure technology networks are segregated into multiple zones according to threat profile. Each zone shall be adequately protected by various security devices including firewall and Intrusion Prevention System (IPS). This must include mobile and wireless networks as well.
5. Ensure security controls for server-to-server external network connections include the following:
   (a) server-to-server authentication such as Public Key Infrastructure (PKI) certificate or user ID and password;
   (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.
6. 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; and
   (d) close relevant ports immediately upon expiry of remote access.
7. Ensure overall network security controls are implemented including the following:
   (a) dedicated firewalls at all segments. All external-facing firewalls must be deployed on High Availability (HA) configuration and “fail-close” mode activated. Deploy different brand name/model for two firewalls located in sequence within the same network path;
   (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-proxy, spam filter and anti-spoofing controls;
   (d) end-point protection solution to detect and remove security threats including viruses and malicious software;
   (e) solution to mitigate advanced persistent threats including zero-day and signatureless malware; and
   (f) capture the full network packets to rebuild relevant network sessions to aid forensics in the event of incidents.
8. Synchronise and protect the Network Time Protocol (NTP) server against tampering.

Appendix 6 Positive List for Enhancements to electronic Banking, Internet Insurance and Internet Takaful Services

Guiding Principles:

1. Does not result in any introduction of new technology to the institution or industry.
2. Does not result in any material change in application architecture or network design.
3. The simplified notification process only applies to enhancements that are explicitly listed below.

Category 1: Notification for Add-on Services to Internet/Mobile Banking/Insurance/Takaful	**Category 2: Notification for Add-on Security Features to Internet/Mobile Banking/Insurance/Takaful**	**Category 3: Notification for Add-on Network/security devices and systems connectivity to approved schemes**
1. Participation in payment gateways involving Financial Process Exchange (FPX), approved payment system operator and registered business (merchant acquiring business) with BNM. 2. Implementation of technology platform approved by Securities Commission e.g. Digital Investment Management 3. Participation in approved schemes as follows: (i) Tabung Haji; (ii) Amanah Saham Nasional Berhad (ASNB); (iii) Skim Simpanan Pendidikan Nasional (SSPN-i); and (iv) PayNet's current and future products and services, e.g. Real-time Retail Payments Platform (RPP) / DuitNow / DuitNow QR, JomPAY and Fasstap	1. Enhance Transaction Authorisation Code (TAC) delivery including subscribing to a new TAC gateway service provider. 2. Enhance the e-Banking system to support migration to Chip and PIN cards. 3. Implement automated storing of privilege IDs. 4. Enhancements to existing login features of biometric security. 5. Enhancement to existing features of MFA method. 6. Enhancement to existing features of phone banking technology. 7. Enhancement on login authentication method on the existing Internet platform.	1. System connectivity with approved schemes i.e. PayNet. 2. Enhancement to add connectivity to third-party service providers i.e. MYEG, Financial Link, Rexit, Bestinet, PSPPA and Merimen. 3. Changes on security and monitoring related tools that include (i) Firewalls; (ii) Intrusion Detection Systems (IDS); and (iii) Intrusion Prevention Systems (IPS). 4. Enhancements of Open API integrations which does not involve the transmission of "confidential" or "sensitive" information.

Guiding Principles:

1. Does not result in any introduction of new technology to the institution or industry.
2. Does not result in any material change in application architecture or network design.
3. The simplified notification process only applies to enhancements that are explicitly listed below.

Category 1: Notification for Add-on Services to Internet/Mobile Banking/Insurance/Takaful	**Category 2: Notification for Add-on Security Features to Internet/Mobile Banking/Insurance/Takaful**	**Category 3: Notification for Add-on Network/security devices and systems connectivity to approved schemes**
4. Enable RENTAS and SWIFT payment transaction initiative on the Internet platform. 5. Participation in existing approved e-channels e.g.: (i) Western Union; (ii) Merchantrade; (iii) Paypal; (iv) Inter Bank Giro (IBG); and (v) Inter Bank Fund Transfer (IBFT). 6. Notification to participate in existing approved e-money issuer. 7. Usage of motor underwriting engine by third-party for calculation of motor premium. 8. Enhancement to application form and underwriting question. 9. Increase in transaction limits including default limit for online/ATM. 10. Enhancement for the following services including new add-on services and features on the existing platform: (i) Debit/credit card activation; (ii) Reset password;		5. Enhancement to add connectivity with approved participants in the Financial Technology Regulatory Sandbox. 6. Enhancement to add connectivity with online distribution channel e.g. telecommunication company. 7. Enhancement to add connectivity with third-party without material change to the existing approved platform. 8. Leveraging approved website/mobile application for e-banking or Internet insurance-related services within financial group.

Guiding Principles: 1. Does not result in any introduction of new technology to the institution or industry. 2. Does not result in any material change in application architecture or network design. 3. The simplified notification process only applies to enhancements that are explicitly listed below.		
Category 1: Notification for Add-on Services to Internet/Mobile Banking/Insurance/Takaful	**Category 2: Notification for Add-on Security Features to Internet/Mobile Banking/Insurance/Takaful**	**Category 3: Notification for Add-on Network/security devices and systems connectivity to approved schemes**
(iii) Block card including enabling debit/credit card for overseas usage; (iv) Credit card PIN change via Internet banking; (v) Credit card activation via SMS/online; (vi) Maintenance of existing product features e.g. time deposit maturity tenor and rates; (vii) Add-on features or services to the existing IVR system; (viii) Add-on features and services from the existing Internet platform to the existing mobile application; (ix) Add-on features and functions to existing approved platform such as loan applications, opening of accounts, purchasing travel/ motor insurance, withdrawal,		

Guiding Principles: 1. Does not result in any introduction of new technology to the institution or industry. 2. Does not result in any material change in application architecture or network design. 3. The simplified notification process only applies to enhancements that are explicitly listed below.		
Category 1: Notification for Add-on Services to Internet/Mobile Banking/Insurance/Takaful	**Category 2: Notification for Add-on Security Features to Internet/Mobile Banking/Insurance/Takaful**	**Category 3: Notification for Add-on Network/security devices and systems connectivity to approved schemes**
surrender, claims and endorsement; (x) Enrolment of new/existing customers onto the online platform; (xi) Maintenance of customer's credential via Internet platform; and (xii) Implementation of "chatbot" or "live chat" onto the existing approved platform to facilitate non-complex activity.		

Appendix 7 Risk Assessment Report

Part A: Financial Institution	
Name of Financial Institution	
Mailing address	
Type of e-banking/Internet insurance and Internet takaful service	New / Enhancement
Description of the e-banking, Internet insurance and Internet takaful service	
Key contact personnel	
Email address	
Phone number	
Part B: External Service Provider	
Name of company	
SSM registration number	
Mailing address	
Engagement period	
Key contact personnel	
Email address	
Phone number	
Part C: 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)

Part D: Technology risk assessment	
Technology risk assessment shall provide assurance on the effectiveness of technology risk control and mitigation performed by the financial institutions in meeting expectations outlined in Part B of Appendix 9	
Part E: Quality assurance	
Overall recommendation	
Part F: Authorised signatory	
Signature	
Name	
Designation	
Date	

Appendix 8 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. e-banking / Internet insurance / Internet takaful * 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 the Guidelines on Internet Insurance (Consolidated) / Circular on Internet Takaful 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 e-banking / Internet insurance / Internet takaful * is subject to appropriate oversight by the board of directors and senior management;
4. appropriate security measures to address e-banking / Internet insurance / Internet takaful * security concerns are in place;
5. customer support services and education related to e-banking / Internet insurance / Internet takaful * are in place;
6. performance monitoring of e-banking / Internet insurance / Internet takaful * products, services, delivery channels and processes has been established;
7. e-banking / Internet insurance / Internet takaful * is included in the contingency and business resumption plans;
8. there are adequate resources to support the offering of e-banking / Internet insurance / Internet takaful * business; and
9. the systems, procedures, security measures, etc. relevant to sound operations of e-banking / Internet insurance / Internet takaful * will constantly be reviewed to keep up with the latest changes.

Signature : ……

Name : ……..

Date : ……..……..

* (*delete whichever is not applicable*)

Appendix 9 Supervisory Expectations on External Party Assurance

Part A: 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 B: 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 should 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.

(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.