BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Risk Management in Technology (RMiT)

Exposure Draft

Applicable to:

1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed international Islamic banks
5. Licensed insurers
6. Licensed takaful operators
7. Licensed international takaful operators
8. Prescribed development financial institutions
9. Eligible issuer of e-money
10. Operator of a designated payment system

Issued on: 4 September 2018 BNM/RH/ED 028-11

This exposure draft sets out the Bank's expectations with regard to financial institutions' technology risk management framework and practices proportionate to the size and complexity of the financial institutions.

Technology risk management is the continuous end to end process of identifying, assessing, mitigating and monitoring related risks to reduce and maintain risk within a predetermined acceptable level. The proposals provide a foundation for the development of an effective risk management programme, necessary for assessing and mitigating risks identified within technology systems. The ultimate goal of the proposals is to help financial institutions better manage technology-related risks and enhance technology resiliency.

The Bank invites written feedback on the proposals in this exposure draft, including suggestions on areas to be clarified and alternative proposals that the Bank should consider. The written feedback should be supported with clear rationale, accompanying evidence or illustrations, as appropriate to facilitate an effective review on this exposure draft.

Responses must be submitted by 31 December 2018 to:

Pengarah
Unit Pakar Risiko dan Penyeliaan IT
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Email: trsu@bnm.gov.my

Electronic submission is encouraged. Submissions received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

In the course of preparing your feedback, you may direct any queries to the following officers at 03-26988044-

a. Zainal Abidin Maarif (ext. 8271)
b. Szazuan Izaham Saat (ext. 8270)
c. Mohd Hosni Che Malik (ext. 7837)
d. Azizi Jefry Abu Bakar (ext. 7847)

Issued on: 4 September 2018

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 Technology risk refers to any risks emanating from information technology (IT) and cyber threats. These risks may arise from failures of IT systems, applications, platforms or infrastructures including threats or vulnerabilities exposed from external network or Internet, which could result in financial loss, disruption of financial services or the operations of the financial institution. Failures or errors in any of the elements above could also lead to adverse reputational impact to the financial institution.

1.2 Technology risk management is the continuous end-to-end process of identifying, assessing, mitigating and monitoring related risks to reduce and maintain risk within a predetermined acceptable level. This policy provides a foundation for the development of an effective risk management programme, necessary for assessing and mitigating risks identified within technology systems. The ultimate goal is to help financial institutions better manage technology risks and enhance technology resiliency.

1.3 Given the increasing enhancement on technology capability coupled with robust pace in product innovations by financial institutions, the Bank had recently implemented a notification based approach for selected low risk enhancements to the e-banking, Internet insurance and Internet takaful services. Subsequently, the Bank has further expanded the notification based approach by requiring all financial institutions to notify the Bank prior to implementing all e-banking/Internet insurance/Internet takaful services (introduction of new technology to the financial institutions or to the industry) or any material enhancements to the existing e-banking/Internet insurance/Internet takaful services.

1.4 This policy document sets out the Bank's expectations with regard to institutions' technology risk management framework and practices proportionate to the size and complexity of the financial institutions.

2 Applicability

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

3 Legal provision

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

(a) Sections 47(1) and 143(1) of the Financial Services Act 2013 (FSA);

(b) Sections 57(1) and 155(1) 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 June 2019.

4.2 The Bank is committed to ensuring that its policies remain relevant and continue to meet the intended objectives and outcome. Accordingly, the Bank will review this policy document within 5 years from the date of issuance or the Bank's last review and, where necessary, amend or replace this policy document.

5 Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, IFSA 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, requirement or specification that must be complied with. Failure to comply may result in one or more enforcement actions;

"G" denotes guidance which may consist of such information, advice or recommendation intended to promote common understanding and sound industry practices which are encouraged to be adopted;

"Approved issuer of e-money" refers to a person approved under section 11 of the FSA or section 11 of the IFSA to issue e-money and for the avoidance of doubt, this may include a banking institution or a non-bank issuer of e-money;

"**Board**" refers to the board of directors of a financial institution;

"Confidential information" or **"sensitive data"** refers to any document or information that is not publicly available either relating to the affairs or account of any customer of a financial institution, or where the document or information relates to a financial institution, disclosure, modification or destruction of the document or information may result in adverse effect on the financial institution's operations, assets, or officers;

"Critical system" refers to application system that supports critical business functions which may involve the following:

(a) Large-value and time-sensitive payment instructions;
(b) Clearing and settlement of material transactions;
(c) Fulfilment of material end-of-day funding and collateral obligations;
(d) Management of banks, customers and counterparties' risk positons;
(e) Provision of essential banking services and payments such as withdrawals, deposits and remittances through various delivery channels that is necessary to maintain public confidence;
(f) Provision of essential insurance/takaful services e.g. e-cover note and issuance of guarantee letter;
(g) Provision of other services that may have systemic impact to other market participants or financial system; and
(h) Regulatory reporting submission;

Question 1 Are there any of your critical systems excluded based on the above definition of critical systems?

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

"Cyber risk" is a type of technology risk which refers to threats or vulnerabilities emanating from connectivity to external networks or the Internet on internal technology infrastructure;

"Designated payment system" refers to a payment system prescribed as a designated payment system under section 30(1) of the FSA or section 39(1) of the IFSA;

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

"Electronic money (e-money)" means a payment instrument or an Islamic payment instrument, whether tangible or intangible, that stores funds electronically in exchange for funds paid to the issuer and is able to be used as a means of making payment to any person other than the issuer;

"Eligible issuer of e-money" means an approved issuer of e-money with substantial market presence based on the criteria set out in accordance with Interoperable Credit Transfer Framework policy document[1];

"Financial institution" refers to:

(a) A licensed person under FSA and IFSA (excluding a professional reinsurer licensed and a professional retakaful operator);
(b) A prescribed development financial institution under the DFIA;
(c) Eligible issuer of e-money; and
(d) Operator of a designated payment system;

[1] An approved issuer of e-money is deemed to have 'substantial market presence' if it fulfils any of the following criteria:
(a) the issuer has at least 500,000 active users (i.e. with at least one financial transaction per month) for a consecutive period of six months;
(b) the issuer has a market share of at least 5% of the total e-money transaction volume or transaction value in Malaysia for a given year beginning 2017;
(c) the issuer has a market share of at least 5% of the total outstanding e-money liabilities in Malaysia for a given year beginning 2017; or
(d) the issuer is an affiliate of an eligible issuer of e-money.

Question 2

The Bank seeks comments on whether the definition of 'financial institution' should be expanded to include eligible issuers of e-money as defined under the Interoperable Credit Transfer Framework. In particular, the Bank seeks views on whether the proposed requirements set out in this Exposure Draft would be proportionate to the nature, scale and complexity of the activities and risk profile of the eligible issuers of e-money. Where relevant, please highlight the following: (i) potential challenges in complying with the proposed requirements; (ii) the specific provisions for which compliance challenges are expected; and (iii) alternative regulatory approaches for the Bank's consideration

Question 3

What would be the key challenges for smaller financial institutions and the locally incorporated foreign institutions which rely on the Group for IT support and services, to comply with the requirements in this exposure draft?

"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 the country through operations of branches and subsidiaries;

"Operator of a designated payment system" refers to any person who operates a designated payment system;

"OTP or One Time Password" refers to a minimum of 6 digit numeric code which is valid only for a 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;

Question 4

Is this definition sufficient to include public cloud services where the risk of contagion arising from multi-tenanted environment is more pervasive such as Amazon Web Services, Microsoft Azure and Google Cloud?

"Production data centre" refers to all facilities hosting active critical production application systems irrespective of location;

"Senior management" refers to the CEO and senior officers; and

"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's software, platform and infrastructure service providers.

6 Related legal instruments and policy documents

6.1 This policy document must be read together with any relevant legal instruments, policy documents 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) Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions[2];
(j) 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) Circular on Internet Takaful.

[2] Subject to the paragraph 7.1(j).

7 Policy documents and circulars superseded

7.1 The policy documents or circulars as listed below are superseded with the coming into effect of this policy document:

(a) Guidelines on Management of IT Environment (GPIS 1) issued in May 2004;

(b) Managing Inherent Risk of Internet Banking Kiosks issued on 5 December 2011;

(c) Preparedness against Distributed Denial of Service Attack issued on 17 October 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) Letter to CEO – 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") dated 7 November 2017;

(g) Letter to CEO - Storage and Transportation of Sensitive Data in Removable Media dated 10 November 2017;

(h) Letter to CEO - 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") dated 17 May 2018;

(i) Letter to CEO – Immediate Measures for Managing identification of Counterfeit Malaysian Currency Notes at Deposit-Accepting Self Service Terminals (SST) dated 31 October 2017; and

(j) Paragraphs 6.1 – 6.4 of the Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions.

PART B POLICY REQUIREMENTS

8 Governance

Board and Senior Management Responsibilities

S 8.1 The Board has overall responsibility for ensuring effective implementation of sound and robust technology risk management for the financial institution to sustain its operations and deliver financial services. In fulfilling this role the Board must provide oversight and guidance in the formulation of the technology risk appetite, strategic plan and other associated risk frameworks commensurate with the nature and complexity of the business.

S 8.2 The Board must review and approve the technology risk appetite and ensure alignment with the financial institutions' risk appetite statement. In doing so, the Board must approve the corresponding risk tolerances for technology related events and ensure key performance and forward looking risk indicators are in place.

S 8.3 The Board must review and approve the IT and cybersecurity strategic plans. These plans must reflect the financial institutions' risk appetite, business and cybersecurity strategy for a period of three to five years. The plans shall provide a comprehensive road-map on technology operations and risk management including requirements on infrastructure, adoption of IT and cyber risk resilience, together with the required resources both financial and non-financial.

S 8.4 These plans shall be periodically reviewed at least biennially commensurate with the complexity of operations and changes in the risk profile as well as business environment.

S 8.5 Technology risk management framework (TRMF) is a framework for safeguarding the financial institution's information infrastructure, systems and data, whilst cyber resilience framework (CRF) is a framework for ensuring the financial institution's cyber resilience. The Board must periodically review and reaffirm the TRMF and CRF at least biennially to guide the financial institution in effectively managing technology risks and to ensure that these frameworks remain relevant on an on-going basis.

S 8.6 The Board must ensure senior management provides sufficiently detailed information on key technology risk and critical technology operations to facilitate strategic decision-making. This includes reporting enterprise key risk indicators on the IT and cyber health posture.

S 8.7 The Board must designate a Board-level committee to provide oversight on overall technology related matters, approve the technology related frameworks including the requirements spelt out in paragraphs 8.2 through 8.6. The chairman of the designated Board committee is also responsible for ensuring the adequacy of ex-ante risk assessment of material technology applications submitted to the Bank.

G 8.8 In promoting effective technology discussions at the Board level, the Board composition should include at least a member with technology experience and competencies.

Question 5
As financial institutions grow increasingly reliant on technology, strategic guidance from the Board members is pivotal. To what extent are financial institutions ready to comply with this requirement if made mandatory?

S 8.9 Given the rapidly evolving cyber threat landscape, the Board shall allocate sufficient time to discuss cyber risks and related issues. The Board shall avail itself to obtain adequate cyber security advice and guidance as appropriate, and continuously engage in cyber security preparedness, education and training. The Board must also understand the strategic reputational risk implications of a cyber incident.

Question 6
How extensive should the Board be educated and trained on cyber security? In this regard, should the Board be engaged by an independent party to determine their level of understanding?

S 8.10 The Board audit committee is responsible for ensuring the effectiveness of the internal technology audit function. This includes ensuring the adequacy of the internal technology audit staff to perform timely and competent technology audits. The Board audit committee must be informed on all corrective actions plan committed and its progress to ensure its timely closure.

S 8.11 Senior management must translate the Board's strategic insights and implement the approved TRMF and CRF into specific policies and procedures within the approved risk appetite and risk tolerance, supported by effective reporting and escalation procedures.

S 8.12 Senior management must establish a dedicated oversight committee to provide strategic and operational guidance on technology. Members of the oversight 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. This includes updates on critical systems' performance, significant IT and cyber incidents, management of technology obsolescent risk, status of patch deployment activities for critical technology infrastructure, progress on strategic technology projects and project approvals, performance of critical technology outsourcing activities and utilisation of technology budget; and

(c) Approve any deviation and exemption for technology-related policies. The committee must ensure robust risk assessment is conducted which is reviewed by risk management committee prior to approval.

S 8.13 Senior management must ensure sufficient allocation of resources to build and support robust technology systems and to maintain competent staff to manage IT operations and cyber risks.

S 8.14 For large financial institutions, senior management must embed appropriate oversight arrangements that focus on technology risk issues within the technology function to support the enterprise-wide oversight of technology risk. These arrangements must also provide for designated staff who do not engage in day-to-day technology operations.

S 8.15 The Bank requires each financial institution to conduct a self-assessment on whether the specific requirements intended for large financial institutions would be relevant to them. The self-assessment shall take into account the institutional risk profile, historical loss data, number of significant business lines within the institution, its market share (e.g. in terms of assets, liabilities, revenue and

premiums), number of subsidiaries, branches and agents, number of transactions, and other business considerations that could give rise to technology risk.

S 8.16 Notwithstanding the self-assessment in paragraph 8.15, where the Bank concludes that a financial institution is a large financial institution, such large financial institution 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 an independent enterprise-wide technology risk management function—

(a) Is made responsible for the implementation of TRMF and CRF; and

(b) Plays an advisory role on critical technology projects, including escalating issues in a timely manner.

S 9.2 A financial institution must designate a Chief Information Security Officer (CISO) to be responsible for the technology risk management function and ensure that the CISO has sufficient authority, independence and resources. The CISO shall—

(a) Be independent from day-to-day technology operations;

(b) Be well aware of current and emerging technology risks affecting the industry which could potentially affect the financial institution's risk profile; and

(c) Be appropriately certified.

Question 7
Given that CISO is entrusted to provide oversight on cyber risk, where would the role be best placed within the financial institution's organisational structure?

S 9.3 The CISO is responsible for ensuring information assets and technologies are adequately protected, which includes the following:

(a) Formulating and facilitating effective implementation of TRMF and CRF;

(b) Enforcing compliance with these frameworks and other technology related regulatory requirements; and

(c) Providing strategic insights on technology risk and security matters as well as the financial institution's technology security risk profile to senior management.

S 9.4 A financial institution must ensure that the TRMF is an integral part of the financial institution's enterprise risk management framework (ERM). The TRMF must include the following:

(a) Clear definition of information technology risk;

(b) Appropriate governance structure and reporting lines;

(c) Identification of technology risks of which the financial institution is exposed to including the adoption of new or emerging technology which may materially alter the risk profile of the financial institution;

(d) Risk classification of all information assets/systems based on its criticality;

(e) Risk measurement and assessment mechanism;

(f) Risk control measures and mitigation plan; and

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

G 9.5 A financial institution should consider the use of automated and advance tools in identifying, monitoring and reporting existing and emerging risk enterprise-wide and tracking of corrective measures.

10 Technology Operations Management

Technology Project Management

S 10.1 A financial institution must establish a robust framework for managing technology projects. The framework shall clearly establish the following:

(a) Project governance including the project oversight, roles and responsibilities, approval requirements, ownership and reporting structure;

(b) Project planning, initiation and implementation strategies that cover feasibility studies including evaluation of acquisition vs in-house developed systems, project timelines and deliverables, resources as well as vendor management where appropriate;

(c) Monitoring and reporting procedures on the project progress, performance and resources;

(d) Escalation process and procedure for resolution of issues to ensure proper deliberation at the appropriate level. Issues that cannot be resolved at the project level shall be escalated to senior management or the designated Board level committee; and

(e) Project closure, comprehensive documentation and post implementation review procedures.

S 10.2 The project team must comprise multiple stakeholders including independent parties with relevant experience and background.

S 10.3 Risk assessment must be conducted as part of the feasibility study and during the life cycle of the technology projects to identify and assess potential technology risks and security threats and to mitigate risk.

S 10.4 An independent quality assurance function shall be established to continuously monitor and instil best practices during the development and deployment of material technology projects.

System Development and Acquisition

G 10.5 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. EAF facilitates the conceptual design and maintenance of the network infrastructure, related technology controls and policies.

S 10.6 A financial institution must adopt appropriate frameworks and risk management practices in their system development life cycle (SDLC) covering system design, development, testing, deployment, change management, maintenance and decommissioning. A financial institution must integrate technology security consideration into the system development process. This framework must be reviewed periodically to be relevant and appropriate to the changing requirements in the development life cycle.

S 10.7 A financial institution must ensure the availability of dedicated SDLC infrastructure to support secure development. This includes the use of automated tools for software development, testing, software deployment, change management, code scanning and software version control.

S 10.8 A financial institution must ensure system design meets user requirements. This includes specifying all necessary components such as hardware and software requirements, transaction data, master files, backups and archives, and interfaces with other systems.

G 10.9 A financial institution is also encouraged to consider diversity in technology to obtain greater resiliency, which may include use of different technology architecture design and application as well as technology platforms and network infrastructure to ensure the critical infrastructure are not exposed to similar technology risk.

S 10.10 A financial institution must ensure that system requirements specified in the detailed design documents are accurately translated to the actual system and the system development process adopts industry recognised standards, where applicable.

S 10.11 A financial institution must establish sound methodology for rigorous system testing prior to deployment to ensure the system meets user requirements and performs robustly. The scope of system testing shall include unit testing, integration testing, user acceptance testing, application security testing, stress and regression testing, exception and negative testing, where applicable. A financial institution shall implement adequate measures to prevent unauthorised disclosure of sensitive test data.

S 10.12 A financial institution shall conduct comprehensive source code review independent of development, prior to introduction of or material changes to critical systems, to ensure the accuracy of system design and functionality, and to identify any security vulnerabilities.

S 10.13 A financial institution must develop risk mitigation plans in cases where the source code of critical technology applications are developed and maintained by vendors. A financial institution must ensure up-to-date source code continues to be readily accessible in the event of discontinued product support or insolvency of the vendor.

S 10.14 A financial institution must establish appropriate process and procedures for system deployment, including the following:

(a) Approval process from relevant stakeholders;

(b) Appropriate controls to mitigate potential technology risks arising from system migration; and

(c) Segregation of duties between development, testing and subsequently production.

S 10.15 A financial institution shall establish three physically segregated environments between production, development and testing for critical systems. Where facilities do not allow for this, logical separation of development and testing environment is allowed only for non-critical systems.

S 10.16 A financial institution must establish a committee comprising representatives of both business and technology to review and approve major business as usual and emergency changes to user and functional system requirements, configurations of network and security devices, and system patches. A financial institution shall establish a contingency plan in the event of unsuccessful implementation of the changes to minimise any business disruptions.

S 10.17 A financial institution must establish appropriate procedures to independently verify changes prior to actual deployment and to ensure no unauthorised changes have been made. Modified programs shall be compared to the authorised change documents to determine that only approved specifications are implemented.

S 10.18 When decommissioning a technology system, a financial institution must prepare a plan to minimise the resulting impact to business operations. The plan shall at minimum include the following:

(a) Impact analysis on the system interaction and dependencies;
(b) Decommissioning strategy;
(c) Migration of existing data;
(d) Archival requirements;
(e) Contingency plan; and
(f) Up-to-date documentation.

S 10.19 A financial institution must implement secured system development and acquisition standards and practices, including the following:

(a) Testing of security controls to ensure its effectiveness prior to implementation;
(b) Implementation of security controls that adhere to current and recognised security standards which may include certification or accreditation where applicable;
(c) Establishment of comprehensive procedures on system edit and validation checking, user access control, system authentication and authorisation, data

integrity checks, logging of system and user activities, and exception handling;

(d) Active monitoring of system and user logs to identify any anomalous activities on the system for further investigation and troubleshooting;

(e) Adequate preservation of information during disposal to conform to legal or regulatory requirements and storage media is sufficiently sanitised to prevent unauthorised leakage of information; and

(f) Periodic review of the effectiveness of security controls in light of possible changes to systems or threats.

Cryptography

S 10.20 A financial institution must establish a robust cryptography policy to protect information as well as promote adoption of strong and consistent cryptographic controls that underpin the digital security of the technology systems and is highly resilient. This policy at minimum shall outline—

(a) Adoption of secure industry standards for encryption algorithms, message authentication and hash functions, digital signatures and random number generation;

(b) Adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction;

(c) Periodic review at least biennially of existing cryptographic standards and algorithms in critical systems, external linked or transactional customer facing applications to prevent exploits of weakened algorithms or protocols; and

(d) Clear roles and responsibilities with regards to policy implementation and key management.

Question 8
What is your institution's current practice to ensure consistent standards are applied with regards to key management and adoption of cryptographic protocols?

S 10.21 A financial institution must undertake a risk assessment to adopt the appropriate cryptographic controls to protect confidentiality, integrity, authentication, authorisation and non-repudiation of information. In addition, a financial institution must consider how the security controls may impact network monitoring visibility and system performance.

S 10.22 A financial institution must ensure the adopted message authentication codes (MAC) functions are resistant to key recovery attacks and are computation resistant. The implementation of MAC must ensure the same key is not reused for message authentication and message encryption.

S 10.23 A financial institution must ensure the adopted hash functions satisfy one-way property and exhibit weak and strong collision resistance.

S 10.24 A financial institution shall implement appropriate digital signature protocol to any document being exchanged electronically. This digital signature protocol must fulfill the conditions of authenticity, non-repudiation and message integrity.

S 10.25 In addition to securely managing secret and private keys, a financial institution must consider the authenticity of public keys. A financial institution must ensure that the authentication process is done using public key certificates, which are normally issued by a certification authority, which shall be a recognised organisation with suitable controls and procedures in place to provide the required degree of trust. A financial institution must also rigorously monitor the expiry of certificates and ensure timely renewal.

S 10.26 A financial institution must consider and select a suitable cryptographically secure pseudo random number generator (PRNG) for the generation of random number given its specific cryptographic purpose e.g. key generation, nonces, one-time pads or salts. The selection must at minimum, consider the following:

(a) Strength of default standard library random number generator function provided by the programming language of operating system;
(b) Use of cryptographically secure PRNG is incorporated into the application;
(c) Proper seeding of PRNG; and
(d) Protection of the seed file where applicable.

S 10.27 A financial institution must adhere to the following:

(a) No key may ever appear on the clear outside the cryptographic device;
(b) Keys must be randomly chosen from the entire keyspace; and
(c) Key-encrypting keys must be separated from data encryption keys.

S 10.28 In addition to the requirement in paragraph 10.27, a large financial institution must implement a fully automated key management system.

S 10.29 Cryptographic keys shall be generated using recognised industry standards' tamper resistant cryptographic module within a secured environment. Unique cryptographic keys shall be generated for single purpose to minimise the impact of compromised keys. These keys should be renewed at appropriate intervals.

S 10.30 Key generation must be secured on premises and not shared with third parties. All key operations must be logged and stored for audit trail purposes, which shall also specify physical controls, logical controls, user access controls and business continuity.

S 10.31 The generated keys shall be transported (when necessary) using secure channels and shall be used by their associated cryptographic algorithm with international cryptographic standards.

S 10.32 A financial institution shall determine the appropriate cryptoperiod for each cryptographic key. The cryptoperiod must take into account key length, key strength, algorithms, and exposure to prevent sensitive data or critical operations from being compromised due to vulnerable cryptographic keys.

S 10.33 A financial institution must ensure storage of cryptographic keys include the following controls:

(a) Keys must be protected on both volatile and persistent memory;
(b) Keys are stored in temper resistant cryptographic vault, such as a hardware security module (HSM);
(c) Keys must be encrypted with Key Encryption Keys (KEKs) prior to the export of the key material. KEK length (and algorithm) must be equivalent to or greater in strength than the keys being protected;
(d) Apply integrity protections while in storage;
(e) No single person have complete access or full knowledge to keys;
(f) Keys are situated in a secure location with restricted access to authorised personnel; and
(g) At minimum, one backup security module must also be located at recovery data centre to ensure business continuity.

S 10.34 A financial institution must establish a secure key backup capability, especially for applications that support data-at-rest encryption for long-term usage. When

backing up keys, ensure that the database that is used to store the keys is encrypted using an industry accepted standard.

S 10.35 When cryptographic keys have expired, a financial institution shall deploy a secure key destruction method to ensure all traces of the keying material are destroyed immediately and cannot be recovered by any parties through physical or electronic means.

S 10.36 A financial institution must establish mechanisms to track and identify users that have access to cryptographic keys throughout their lifecycles. The key management system shall account for all individuals who are able to view plaintext cryptographic keys.

S 10.37 A financial institution must establish a compromise-recovery plan in the event of a key compromise. The compromise-recovery plan shall contain:

(a) Impact assessment;
(b) Escalation process;
(c) Keys regeneration;
(d) Interim measures; and
(e) Business as usual.

Data Centre Resiliency

Data Centre Infrastructure

S 10.38 A financial institution must articulate and align the resiliency and availability objectives of its data centres with 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. Financial institutions must establish appropriate governance and controls to mitigate associated risks where it relies on external service providers.

S 10.39 A financial institution must ensure production data centres meet international standards equivalent to at least Tier-III requirements.

Question 9
What would be the key challenges for small financial institutions to ensure its production data centres must meet international standards equivalent to at least Tier-III requirements?

S 10.40 In addition to the requirement in paragraph 10.39, large financial institutions are also required to ensure recovery data centres meet international standards equivalent to at least Tier-III requirements.

S 10.41 A financial institution must ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centres which includes the following:

(a) Hardware such as servers, storage, network equipment and security devices; and

(b) Electrical utilities such as uninterruptable power supply (UPS) and power transfer switches.

S 10.42 Production data centres must be hosted in purpose-built facilities intended for data centre usage and not located in a disaster prone area. At a minimum, these facilities must provide:

(a) Dedicated power supply and telecommunication lines;

(b) Security-centric design taking into consideration the internal and external threats, including physical security layout, monitoring and surveillance;

(c) Enforcement of stringent physical access controls with layered defence parameter;

(d) Proper environmental and safety control settings such as cooling and fire suppression systems; and

(e) Certification on security management of data centre by internationally recognised professional body.

S 10.43 Production data centres must deploy integrated data centre infrastructure management system that provides unified view of the data centre infrastructure health in real-time with timely alerts on faults as well as indicators of potential issues. This includes monitoring of the server rooms and individual server racks' temperature, UPS and its individual battery cells.

S 10.44 A financial institution operating its production data centres on shared third party facilities must ensure the following:

(a) Dedicated secured space with proper caging for its server and equipment racks;

(b) For shared critical power equipment, clearly document the arrangement for power allocation between tenants in the service level agreements including prioritisation given to the financial institution during power outages; and

(c) Adequate power capacity and physical space are available for future technology system expansion.

S 10.45 A financial institution is required to appoint a technically competent external service provider to carry out regular production data centre resiliency and risk assessment (DCRA) and set proportionate controls aligned with its enterprise risk appetite. The assessment must consider all major risks and determine its current level of resiliency. The assessment shall include adherence to the requirements in paragraphs 10.39 to 10.44 at minimum.

S 10.46 A financial institution must ensure that the assessment in paragraph 10.45 above is conducted at least biennially. The designated board committee must deliberate and endorse the outcome of the assessment.

G 10.47 A financial institution operating its data centres on shared facilities should ensure the service provider does not host more than 30% of all financial institutions within a single facility to mitigate concentration risk.

Data Centre Operations

S 10.48 A financial institution must establish a comprehensive and forward looking capacity management plan commensurate with its potential future business growth plans. This includes ensuring adequate system storage, central processing unit (CPU) power, memory and network bandwidth. This exercise shall involve both technology and relevant business stakeholders.

S 10.49 A financial institution must establish real-time application and infrastructure monitoring systems to track capacity utilisation and performance of key processes and services. This monitoring system shall:

(a) Run independently from production services;

(b) Not degrade the performance of the monitored system; and

(c) Provide timely and actionable alerts to administrators.

S 10.50 A financial institution must ensure the existence of a regular programmes of preventive maintenance on all technology systems and infrastructure components.

Such maintenance work shall not unduly affect the availability and quality of banking and insurance services provided.

S 10.51 A financial institution must ensure that segregation of incompatible duties is implemented in the data centre operations environment to prevent operators from performing any unauthorised tasks. In the case where vendors' or programmers' access to the production environment is necessary, all their activities must also be properly authorised and monitored.

S 10.52 A financial institution must establish adequate control procedures and deploy automated tools for batch processing management to ensure timely and accurate batch processes. These include changes in the production system, error handling management as well as other exceptional conditions. A financial institution shall subject ad-hoc batch jobs to stringent checks and testing to ensure it does not impact the availability of critical systems and integrity of the information processed.

S 10.53 A financial institution must maintain sufficient number of backup copies of critical data, the updated version of the operating system software, production programs, system utilities and all master and transaction files as well as event logs for recovery purposes. Backup media must be stored in an environmentally secure and access-controlled dedicated backup site.

S 10.54 A financial institution is required to conduct an independent risk assessment on its end-to-end backup storage and delivery management in ensuring existing controls are adequate in protecting sensitive data at all times. In this regards, financial institution is also required to adhere to the requirements specified in Appendix 1.

S 10.55 A financial institution must ensure each critical system and its interfaces are designed for high availability and must not exceed cumulative unplanned downtime of more than 4 hours on a rolling 12 months basis and maximum 90 minutes downtime per incident.

Question 10
What would be the key challenges to ensure critical systems do not exceed cumulative unplanned downtime of more than 4 hours and maximum 90 minutes downtime per incident? What would be the estimated time needed to implement these new requirements?

Network Resiliency

S 10.56 A financial institution must design a reliable, scalable and secure enterprise network to ensure it is able to provide and maintain a robust level of network services.

S 10.57 A financial institution must ensure the reliability of network services by implementing appropriate component redundancy and service diversity to protect against potential network faults and cyber threats. This includes the following:

(a) Deploying redundant interfaces, backup modules and standby devices;

(b) Implementing alternate network paths for critical systems;

(c) Engaging alternate Internet service provider (ISP) in addition to the main ISP for online services; and

(d) Implementing cross-border network redundancy.

S 10.58 A financial institution must ensure the scalability of network services and protocols, and that monitoring tools are taken into consideration during the design stage commensurate with business growth expectations.

S 10.59 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 as well as traffic anomalies.

S 10.60 A financial institution must ensure network services are designed and implemented with security in mind to ensure confidentiality, integrity, and availability of data and system resources supporting critical business functions.

S 10.61 A financial institution must establish network policies and procedures to govern the network operation, configuration, security setup and incident handling programmes including processes for approving, testing, installing, and documenting network changes.

S 10.62 A financial institution must establish and maintain a network design blueprint encompassing all of its internal and external network interfaces and connectivity. The blueprint must highlight physical and logical connectivity between network components and network segmentations.

S 10.63 A financial institution must establish contractual agreements with the network service providers which clearly stipulate the roles and responsibilities of parties involved, service levels and non-disclosure agreements, continuity of service, as well as logical and physical security controls to be implemented.

S 10.64 A financial institution must ensure sufficient network devices logs are retained for audit reviews and investigations up to at least 3 years.

S 10.65 A financial institution must establish logical network segmentation for the financial institution separate from other entities or subsidiaries within the same group to minimise the risk of a system compromise in one entity affecting other entities within the same network segment.

G 10.66 A financial institution should establish dedicated switches for critical systems separate from the general technology environment of the entity.

S 10.67 A financial institution must engage an external independent party to perform network resiliency and risk assessments (NRA) to identify issues, analyse the issues and recommend measures to ensure network resiliency. A financial institution is required to conduct subsequent NRAs whenever there is a material change in the network design.

Third Party Service Provider Management

S 10.68 The Board and senior management of the financial institution must exercise effective oversight and address associated risks when outsourcing critical technology functions and systems. Engagement of third party service providers does not eliminate the accountabilities and responsibilities of financial institutions.

S 10.69 A financial institution must conduct due diligence on the third party service provider's competency, system infrastructure and financial viability prior to engaging its services. Due diligence must include assessment on the service provider's capabilities to manage all risks including the following:

(a) Data leakage including unauthorised disclosure of confidential data due to data co-mingling;

(b) Service disruption including capacity performance;

(c) Processing error;

(d) Physical security breaches;

(e) Cyber threats;
(f) Over-reliance on key personnel; and
(g) Security measures implemented on transmission, processing, storage or handling of confidential information pertaining to the financial institution or its customers.

S 10.70 A financial institution must establish service-level agreement (SLA) when engaging third party service providers. At the minimum, the SLA shall contain the following:

(a) Access rights to regulator and any party appointed by the financial institution to examine any activity or entity of the financial institution, as well as to access any records, files or data of the financial institution, including management information and the minutes of all consultative and decision-making process;
(b) Any material changes that may affect a financial institution's outsourced functions and any sub-contracting of critical work must obtain approval from the financial institution;
(c) Service provider shall provide sufficient prior notice to financial institutions of any sub-contracting of critical work;
(d) Written undertaking on compliance with secrecy provisions as provided by the relevant legislation;
(e) Arrangements for disaster recovery and backup capability, where applicable;
(f) Critical system availability; and
(g) Exit and termination clause.

S 10.71 A financial institution must regularly review the SLA with its third party service provider to ensure the services provided is commensurate with the latest security and technological developments.

S 10.72 A financial institution must ensure its third party service providers comply with all relevant regulatory requirements prescribed in this policy document. This includes specific requirements for system development and acquisition, data centre operations, network resiliency, technology security and cybersecurity, wherever applicable.

S 10.73 A financial institution must ensure data residing in third party service providers are recoverable timely and failure of the third party service provider will not lead to

systemic impact. In the event of cyber incident, a financial institution must initiate prompt update and disclosure to relevant regulatory bodies.

S 10.74 A financial institution must ensure that storage of its data is clearly segregated from the other clients of the third party service provider. There shall be proper control and periodic review of the access provided to authorised users.

S 10.75 A financial institution must establish contingency plans in case of non-performance or unsatisfactory performance by the third party service provider.

Cloud Services

S 10.76 A financial institution shall not rely on public cloud computing services to manage, operate or host critical technology functions, systems and confidential information.

S 10.77 A financial institution must fully understand the inherent risk of adopting cloud services. In this regard, a financial institution is required to conduct risk assessment prior to cloud adoption which considers the inherent architecture of cloud services which rely on sharing of resources and services across multiple tenants over the Internet. This risk assessment must include consideration of the following:

(a) Sophistication of the deployment model;
(b) Migration of existing system to cloud infrastructure;
(c) Location of cloud infrastructure;
(d) Multi-tenancy or data co-mingling;
(e) Vendor lock-in, application portability or interoperability;
(f) Ability to customise security configurations of the cloud infrastructure to ensure high level of data and technology system protection;
(g) Exposure to cyber-attacks via cloud service providers;
(h) Exit strategy including data removal and deletion;
(i) Demarcation of responsibilities, limitations and liability of the service provider; and
(j) Compliance to regulatory requirements and international standards on cloud computing.

S 10.78 A financial institution must ensure the following minimum requirements are implemented to manage the use of confidential information:

(a) Deploy on-premises data loss prevention (DLP) to protect confidential information;

(b) Strong encryption standard with the encryption key(s) held solely by the financial institution;

(c) Enforce logical separation of data from other clients of the cloud provider to mitigate risk of co-mingling in multi-tenanted environments; and

(d) Deploy stronger multi-factor authentication for privileged access and rights management system where the security administrator function is managed by the financial institution.

Question 11 How best to ensure logical segregation of confidential data in multi-tenanted environment?

Access Control

S 10.79 A financial institution must establish an effective access control policy to manage the risk of unauthorised access to its technology systems. The access control policy must include logical and physical technology access controls of its users (including external users e.g. third party service providers), technology systems and technology assets.

S 10.80 A financial institution must reflect the following principles in its access control policy:

(a) Adopt a "deny all" access control policy for users by default unless explicitly authorised;

(b) Enforce "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 such as—

(i) System development and technology operations;

(ii) Security administration and system administration; and

(iii) Network operation and network security.

(e) Enforce dual control functions which requires two or more persons to execute an activity;

(f) Adopt stronger authentication for critical activities including for remote access;

(g) Prohibit use of same user ID for multiple concurrent sessions;

(h) Prohibit sharing of user ID and passwords across multiple users; and

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

S 10.81 A financial institution must have in place robust identification process to identify users. This includes background screening before assigning access to any user. More rigorous and thorough screening is expected to be performed for critical or security roles and responsibilities.

S 10.82 A financial institution must employ robust authentication processes to ensure the identity in use is authentic. Authentication methodologies shall be commensurate with the criticality of the functions by adopting 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 10.83 A financial institution shall continuously review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There must be a mechanism to automatically generate passwords and to check the strength of the passwords created manually.

G 10.84 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) multifactor authentication methodologies that are more reliable indicators of authentication and stronger fraud deterrents.

G 10.85 A financial institution is encouraged to adopt dedicated user domains for selected critical functions, separate from the broader enterprise-wide user authentication system.

S 10.86 A financial institution must establish a user access matrix to outline the access rights, roles or profile, as well as authorising and approving authorities. The access matrix must be periodically reviewed and updated.

S 10.87 A financial institution must ensure access controls to common technology systems are effectively managed and monitored.

S 10.88 In fulfilling the requirement under paragraph 10.87, large financial institutions are required to deploy an identity access management system to effectively manage and monitor user access to common technology systems.

S 10.89 A financial institution must not allow remote access by default. Should remote access be required and granted, the principles outlined in paragraph 10.80 must be applied.

S 10.90 A financial institution must ensure all user activities are logged and periodically reviewed.

S 10.91 In addition to the requirement under paragraph 10.90, large financial institutions are required to deploy automated audit tools to flag any anomalies.

Patch and End-of-Life System Management

S 10.92 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.

S 10.93 A financial institution must establish functions to continuously monitor and implement latest patch releases in a timely manner and identify critical technology systems that are approaching EOL for further remedial action.

S 10.94 In fulfilling the objective under paragraph 10.93, large financial institutions must establish a dedicated function.

S 10.95 A financial institution must establish a patch and EOL management framework which outlines amongst others the following:

(a) Identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems;

(b) Conduct compatibility testing for critical patches;

(c) Specified turnaround time according to the severity of the patches; and

(d) Workflow of end-to-end patch deployment processes including approval, monitoring and tracking of activities.

Security of Digital Services

S 10.96 A financial institution must implement robust technology security controls in providing digital services based on the following key principles:

(a) Confidentiality and integrity of customer information and transaction;

(b) Reliability of services delivered via channels and devices;

(c) Proper authentication of users or devices and authorisation of transactions;

(d) Minimum disruption to services;

(e) Sufficient audit trail and anomalous transaction monitoring;

(f) Fall back transaction recovery mechanisms; and

(g) Strong physical control and logical control measures.

S 10.97 A financial institution must implement controls to authenticate and monitor all financial transactions. These controls at minimum must be able to mitigate man-in-the-middle attacks, transaction fraud, phishing and compromise of application systems and information.

Question 12
The Bank seeks comments on whether single factor authentication (1FA) should be allowed for low-value transactions subject to appropriate safeguards (e.g. transaction limits and the facility for users to lower or zerorise such limits). This is intended to promote proportionate regulation, while fostering a more enabling environment for the adoption of emerging e-payment methods such as mobile payments. Where 1FA is allowed for low-value transactions, the Bank also seeks views on whether the Bank should prescribe the threshold for "low-value transactions", and/or the specific type of 1FA permissible for such transactions?

S 10.98 A financial institution must implement additional controls to authenticate devices and users, authorise transactions as well as support non-repudiation and accountability for high-risk transactions. These measures must include 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) Strong multi-factor authentication for transactions proportionate to the level of risk such as larger value fund transfers or abnormal transaction behavior;
(d) If OTP is used as a second factor, it must be dynamic and time based;
(e) Request the users to verify details of transaction prior to execution;
(f) Secure user and session handling management;
(g) Proof of origin and destination, as well as transaction data integrity;
(h) Strong mutual authentication between the users' end-point devices and financial institutions' servers, including the use of latest version of Extended Validation SSL certificate (EV SSL);
(i) Timely alerts of suspicious transactions through implementation of monitoring system; and
(j) Timely notification to customers that is sufficiently descriptive on the nature of transaction.

S 10.99 A financial institution shall ensure sufficient tamper resistant digital services logs are retained for audit reviews and investigations up to at least 3 years.

S 10.100 A financial institution must ensure system performance, availability and recovery capability of its digital services is proportionate to the importance of the digital services offered. In particular, critical online banking[3] as well as online insurance[4] services must have high availability with reasonable response time including page load time.

S 10.101 A financial institution must ensure adequate tracking mechanisms and operational processes are in place to handle incomplete transmission of data such as those caused by time-outs or interruption of power supply which could lead to "account debited, money not transferred" incidences.

G 10.102 A financial institution should use more secure two-factor authentication (2FA) methods than unencrypted short messaging service (SMS) by deploying more secure technology and channels.

S 10.103 A financial institution must ensure OTPs generated via soft or hard token is adequately secured, which includes the following:

[3] Internet and mobile banking
[4] Issuance of electronic cover note for motor insurance and takaful and issuance of guarantee letter for life insurance and family takaful

(a) Binding the token to the customer's account;

(b) Activation of tokens must be subject to multi-factor authentication by the customer;

(c) Assigning a customer to only a single soft and/or hard token; and

(d) Timely notification to customers of any activation and changes of token device via customer's verified communication channel such as SMS.

S 10.104 A financial institution shall deploy stronger two-factor authentication solutions for open third party fund transfer for transactions with a value of RM10,000 and above with the following additional features:

(a) Binding the transaction details to the OTP generated by the device (e.g. beneficiary account number, amount of transaction);

(b) Generating the OTP from the customer's device and not from the bank's server; and

(c) Requiring the customer to physically key in the generated OTP into the application.

Question 13
As the industry average for fund transfers exceeding RM10,000 are generally well below 10%, should stronger 2FA be extended to other high risks transactions e.g. registration of favourite beneficiaries, to ensure customers are well protected?

S 10.105 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[5] must comply with internationally recognised standards where available. The advance technology must be resilient against cyber threats[6] including malware, phishing or data leakage.

S 10.106 A financial institution must undertake a comprehensive risk assessment of the advanced technologies and the algorithms deployed in their digital services to mitigate associated risks. Algorithms must be regularly reviewed and validated to ensure they remain appropriate and accurate.

[5] Such as Quick Response (QR) code, Bar Code, Near Field Communication (NFC), Radio Frequency Identification (RFID), Wearables.

[6] For example, in respect of QR payments, financial institutions shall implement safeguards within their respective mobile applications to detect and mitigate risks relating to QR code that may contain malware or links to phishing websites.

S 10.107 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.

S 10.108 A financial institution must perform continuous surveillance to assess the security vulnerability of the operating system used for the digital delivery channels and implement appropriate corresponding safeguards particularly for mobile applications. In addition, a financial institution shall also comply with the requirements specified for each digital delivery channel in Appendices 2 to 4, where relevant.

11 Cybersecurity Management

Cyber Risk Management

S 11.1 A financial institution must ensure that there is enterprise-wide focus for effective cyber risk management as it is a collective responsibility of business and technology lines. In addition to the Board's responsibilities in paragraph 8.5, the Board must provide proactive oversight and ensure relevant stakeholders are involved in the development and implementation of CRF.

S 11.2 A financial institution must develop a CRF which clearly articulates the institution's cyber resiliency objectives and its risk tolerance amidst a constantly evolving cyber threat environment. The framework must be able to support effective identification, protection, detection, response, and recovery (IPDRR) from internal as well as external cyber-attacks.

S 11.3 A financial institution must ensure that its CRF must consist at minimum the following elements:

(a) Development of institutional understanding of the overall cyber risk context, its exposure and current cybersecurity posture;

(b) Identification, classification and prioritisation of critical systems, information, assets and interconnectivity (internal and external parties) to obtain a complete and accurate view of its information assets, systems, interdependencies and risk profile;

(c) Identification of cybersecurity threats and its countermeasures including brand protection mechanisms;

Question 14 Is your financial institution already subscribing to a brand protection services? If not, what are the measures currently deployed to protect your financial institution's digital footprint?

(d) Implement layered (defense-in-depth) security controls to protect its data, infrastructure and assets against evolving threats;

(e) Implement timely detection mechanism of cybersecurity events through continuous surveillance and monitoring;

(f) Develop comprehensive incident handling and crisis response management playbook, plans and activities to contain any damage resulting from a cybersecurity breach;

(g) Develop and implement recovery procedures from cyber incidents including development of appropriate plans and activities to resume normal operations in a timely manner; and

(h) Promote collaboration, timely and secure information sharing between industry players to strengthen cyber resilience.

S 11.4 In addition to the requirements in paragraph 11.3 above, a large financial institution is required to implement a centralised automated tracking system to manage its technology asset inventory under its CRF.

S 11.5 A large financial institution must establish a dedicated in-house cyber risk function to manage cyber risks and respond to potential cyber-attacks. The cyber risk function shall be responsible for the following:

(a) Perform detailed analysis on cyber threats, provide risk assessment on potential cyber-attacks and ensure timely review and escalation of all high risk cyber threats to senior management; and

(b) Proactively test and simulate sophisticated "Red Team" attacks on its current security controls and identify potential vulnerabilities including infrastructure hosted with third party service providers.

Cybersecurity Operations

S 11.6 A financial institution must establish a cybersecurity function responsible for implementing cybersecurity controls including at minimum the measures specified in Appendix 5**.** A financial institution must fully understand the cyber-attack lifecycle and implement appropriate mitigating measures. The cyber-attack lifecycle must include the following phases:

(a) Reconnaissance;

(b) Weaponisation;

(c) Delivery;

(d) Exploitation;

(e) Installation;

(f) Command and control; and

(g) Exfiltration.

S 11.7 A financial institution must enable continuous and proactive monitoring and deploy advanced tools to timely detect anomalous activities in its technology infrastructure. The scope of monitoring must be extensive to cover all critical technology applications and systems including its supporting infrastructure.

S 11.8 A financial institution must continuously assess its security posture to provide reliable assurance of its resiliency against sophisticated threats and vulnerabilities.

S 11.9 A financial institution must conduct annual intelligence-led penetration testing on the internal and external network infrastructure as well as the critical application system including web, mobile and all external facing application. The penetration testing should reflect extreme but plausible cyberattack scenarios based on emerging and evolving threat landscape. A financial institution must engage suitably accredited penetration testers and service providers to perform this function.

S 11.10 A large financial institution must undertake independent compromise assessment on its critical technology infrastructure at least annually.

S 11.11 A large financial institution must establish an internal security function (Blue Team) within the financial institution’s technology department to continuously detect, defend and prevent potential compromise of its security controls or weakening of

its security posture. This includes performing quarterly vulnerability assessment of external and internal network components that support all critical systems.

Question 15
As the role of the Red Team is to proactively test existing control measures and identify weaknesses, whilst the Blue Team's role is to ensure security controls are working correctly, where should these teams be situated within the organisation structure? Given both functions must remain sufficiently independent from each other, should the teams be established within different lines of defense?

S 11.12 A financial institution must establish standard operating procedures (SOP) for vulnerability assessment and penetration testing (VAPT) activities. The SOP must spell out the relevant control measures including ensuring the external penetration testers are accompanied in-premise at all times, validating the event logs and ensuring data purging.

S 11.13 A financial institution must ensure penetration testing results are timely escalated to senior management. A financial institution must require the penetration testing vendor to submit a comprehensive report with remedial action to senior management.

Distributed Denial of Service (DDoS)

S 11.14 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 volumetric, protocol and application layer DDoS attacks by carrying out the following measures:

(a) Subscribe 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 assess the capability of the provider to expand network bandwidth on demand including upstream provider capability, adequacy of its incident response plan and its responsiveness to an attack;

(c) Engage at least one backup ISP in addition to the main ISP;

(d) Ensure timely update of DDoS attack signatures on security devices;

(e) Implement Web Application Firewall (WAF) to mitigate against application layer attacks;

(f) Implement mechanism to mitigate against DNS based layer attacks; and

(g) Enable detection of DDoS attack via deep packet analysis.

Data Loss Prevention (DLP)

S 11.15 A financial institution must establish clear DLP process and strategy in order to ensure that important data is identified, classified and secured. At minimum, a financial institution must comply with the following:

(a) A financial institution shall ensure that data owners are accountable and responsible for identifying and classifying their data adequately. A financial institution is required to undertake a data discovery process prior to development of data classification scheme and data inventory; and

(b) A financial institution must ensure that data accessible by third parties is identified and policy must be implemented to safeguard third party access. An agreement must be in place to ensure interests of the financial institutions are adequately protected.

S 11.16 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. At minimum the technology deployed must cover the following:

(a) Data in-use – data residing in computers, external/removable devices and end point devices;

(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 11.17 Proper data removal approach must be implemented on technology equipment, mobile devices or storage media that have been designated to be discontinued by the financial institution, by adopting proven data wipe and sanitisation techniques. For mobile devices that are not owned by the financial institution, a remote uninstallation and data wipe capabilities must also be established and used on identified devices, especially when a previously appointed person is deemed no longer authorised by the institution.

Security Operations Centre (SOC)

S 11.18 A financial institution must establish SOC capabilities for proactive monitoring of its technology security posture to detect anomalous user or network activities, flag potential breaches and establish appropriate response.

S 11.19 The functions of SOC must include log collection and event correlation engine with parameter driven use cases such as Security Information and Event Management (SIEM), incident coordination and response mechanism including use of automated incident and case management engine with multi-tiered dedicated skilled resources for real time monitoring and triage.

S 11.20 A financial institution must also ensure the following functions are performed to further enhance the SOC's capabilities:

(a) Vulnerability management including conducting vulnerability assessment, penetration testing and threat hunting;

(b) Remediation functions including ability to perform forensics artifact handling, malware and implant analysis; and

(c) Provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, monitoring indicators of compromise (IOC). This includes advanced behavioural analysis to detect signature-less malware or identify anomalies that may pose security threats.

Question 16 Does your current SOC capabilities, in-house or otherwise, include machine-learning capabilities to automatically flag for advanced persistent threats?

S 11.21 A financial institution must undertake regular review on strategy, update of monitoring scope and requirements of the SOC.

S 11.22 A financial institution must ensure that the SOC provides a threat assessment report at least monthly which at minimum, includes the following:

(a) Trends and statistics based on 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.

S 11.23 A financial institution must subscribe to reputable threat intelligence services to identify emerging cyber threats, uncover new cyber-attack techniques and provide counter measures.

S 11.24 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;

(c) The SOC has a holistic and end-to-end view of the financial institution's infrastructure including internal and external facing perimeters; and

(d) The SIEM must be able to normalise and correlate security and event logs on timely basis from all servers, security and network devices at all sites such as data centre, secondary data centre, disaster recovery centre, head office and branches.

Cyber Response and Recovery

S 11.25 A financial institution must establish comprehensive cyber crisis management policies and procedures as well as incorporate cyber-attack scenarios and preparedness in the organisation's overall crisis management plan, escalation processes, business continuity and disaster recovery planning.

S 11.26 A financial institution must develop a clear communication plan to shareholders, regulatory authorities, customers and employees in the event of a cyber incident.

S 11.27 A financial institution must establish a comprehensive Cyber Incident Response Plan (CIRP). The CIRP must include the following elements:

(a) Preparation

Design and implement a resilient CIRP incorporating governance process, reporting structure, role 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

Implement mechanism to proactively monitor its technology infrastructure incorporating relevant threat intelligence and to continuously validate the security posture of its network environment. Identify points of compromise, determine extent of damage and ensure sufficient evidence is preserved for forensics purposes;

(c) Containment, eradication and recovery

Undertake risk-remedial actions to prevent damage to the financial institutions, remove the known threats and resume business activities; and

(d) Post-incident activity

Conduct post-incident assessment review incorporating lessons learned and develop long-term risk mitigation.

S 11.28 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. Key contact person and his/her alternate must be appointed to liaise with the Bank during an incident.

S 11.29 A financial institution must conduct annual cyber drill exercise to test the effectiveness of CIRP based on various current and emerging threat scenarios (e.g. social engineering) with the involvement of key stakeholders including members of senior management, the Board and third party service providers.

S 11.30 A financial institution must ensure the CIRP is tested periodically. The test scenarios must include:

a) Escalation processes to assess the effectiveness of communication and decision-making based on the level of impact of a cyber incident; and
b) Readiness and effectiveness of CERT including relevant third party service providers required to support the recovery process.

S 11.31 A financial institution must immediately notify the Bank of any cyber incidents affecting the institution. Upon completion of investigation, the financial institution is also required to submit a report on the incident as specified in ORION[7].

G 11.32 A financial institution is highly encouraged to ensure active information sharing by establishing close collaboration and cooperation with relevant stakeholders and competent authorities on combating cyber threats and sharing of mitigation measures.

12 Technology Audit

S 12.1 A financial institution must ensure that the scope, frequency and intensity of technology audit commensurate with the complexity, sophistication and criticality of technology systems and applications.

S 12.2 A financial institution must ensure internal audit has relevant technology audit competencies and is familiar with the financial institution's technology operations.

[7] Operational Risk Integrated Online Network

S 12.3 Notwithstanding 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.

S 12.4 A financial institution must ensure that the technology audit plan includes critical technology services, third party service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post implementation review of new or material enhancements of technology services.

S 12.5 The financial institution shall ensure that internal audit function (in the case of paragraph 12.2) and the dedicated internal technology audit (in the case of paragraph 12.3) shall act as an independent party to provide views in an advisory capacity on the compliance and adequacy of control processes during planning and development of new major products, systems or technology operations. The technology auditors participating in this capacity shall not perform the post implementation review.

13 Internal Awareness and Training

S 13.1 A financial institution must provide adequate and regular technology and cybersecurity awareness education (such as measures to mitigate social engineering attacks) for all staff in undertaking their respective roles. A financial institution must establish mechanisms to measure the effectiveness of the training. This cybersecurity awareness education must reflect current cyber threats landscape and to be conducted at least annually.

S 13.2 A financial institution must provide adequate training to continuously enhance technology operations, cyber security and risk management staff's technical competencies and capacity commensurate with the requirements of 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 are also suitably certified.

S 13.4 A financial institution must ensure internal technology audit staff are professionally certified and provided with the necessary training to keep abreast with the

developing sophistication in the financial institution's technology system and delivery channels.

Question 17
To ensure technology audit is performing competently and comprehensively, what would be the ideal transition period to ensure all staff are professionally certified?

S 13.5 A financial institution must ensure its Board members undergo regular training in order to understand and appreciate technology risk.

PART C REGULATORY PROCESS

14 Notification for Technology Related Application

S 14.1 A financial institution must notify the Bank in accordance with the requirements in this Part C prior to conducting e-banking, Internet insurance and Internet takaful services[8], including introducing new technology relating to e-banking, Internet insurance and Internet takaful.

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

(a) Strategic plan as to how the financial institution would be providing e-banking, Internet insurance and Internet takaful services. This includes specific accountabilities, policies and controls to address risks;

(b) Security arrangements and control;

(c) 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 listed in Appendix 6 (Positive List) or constitutes other enhancements not listed in the Positive List. The Positive 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 impact and risk mitigation.

[8] The meaning of the terms “e-banking”, “Internet insurance” and “Internet takaful” is in accordance with:
(i) Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions;
(ii) Guidelines on Internet Insurance (Consolidated); and
(iii) Circular on Internet Takaful, as the case may be.

S 14.5 For any enhancements 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 a declaration that the financial institution has addressed associated technology risks and security controls on 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 declaration is set out in Appendix 9; and

b) Provide a confirmation by management senior officer of the financial institution which is attested by the Chairman of the designated Board committee as stipulated in paragraph 8.7. The attestation must clearly state that the financial institution has observed the guidelines and circular as stated in paragraph 14.1 and is ready to provide e-banking, Internet insurance and Internet takaful services or any material enhancement to the e-banking, Internet insurance and Internet takaful services. The format of the confirmation is set out in Appendix 7.

S 14.6 A financial institution must ensure that the independent external party providing the declaration under paragraph 14.5(a) is competent, with a good track record. The Bank expects the independent external party to provide an objective and independent declaration to the Bank that the financial institution has adequately addressed all potential risks and put in place effective security controls in offering new e-banking, Internet insurance and Internet takaful services or any material enhancement to the e-banking, Internet insurance and Internet takaful services. The Bank's expectations on the external party providing the declaration are as outlined in Appendix 8.

G 14.7 Upon submission of the notification under paragraph 14.1 and compliance with the requirements in this Part C (Regulatory Process), a financial institution may conduct the e-banking, Internet insurance and Internet takaful services or implement any enhancement to the services immediately.

PART D SUPERVISORY AND ADMINISTRATIVE ACTIONS

15 Supervisory and Administrative Actions

G 15.1 Appropriate supervisory and administrative actions may be taken by the Bank in accordance with the law for the financial institution's failure to meet the requirements under this policy document, which may include—

(a) Subjecting any services offered by the financial institution to the prior review or specific approval of the Bank before the services may be offered;

(b) Directing the financial institution to suspend or cease any services offered;

(c) Directing the financial institution to compensate consumers that have suffered losses;

(d) Directing the financial institution to modify the terms and conditions of any services offered; or

(e) Publishing details of corrective actions taken against the financial institution.

Appendix 1

Storage and Transportation of Sensitive Data in Removable Media

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

1. Deploy latest industry-tested and accepted encryption techniques;
2. Implement authorised access control to sensitive data (e.g. password protection, user access matrix);
3. Prohibit 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 chain of custody process for media management which include:
        (i) Media must not be under single custody at any point of time;
        (ii) Media must always be within sight of the designated custodians; and
        (iii) 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. Ensure third party service providers complied with the requirements in paragraphs 1 to 4 of Appendix 1, in the event third party services are required in undertaking the storage management or transportation process of sensitive data.

Appendix 2

Minimum Control Measures on Self-service Terminals (SSTs)

Cash SST

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

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

1. Enforce full hard disk encryption;

2. Retain 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. Ensure Cash SST operating system is running on secured version operating system with continued developer or vendor support for security patches to fix any operating system security and vulnerabilities;

4. Deploy Anti-virus (AV) solution for Cash SST and ensure timely update of signatures. Ensure virus scanning on all Cash SSTs is performed periodically;

5. Implement centralised management system to monitor and alert any unauthorised activities on Cash SST such as unauthorised shutting-down of OS or deactivation of white-listing programme;

6. Ensure effective control over the Cash SST lock and key by using 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. Install 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. Secure physically the Cash SST PC Core by enclosing the CPU in a locked case;

9. Enforce firewall and Intrusion Prevention System (IPS) at the financial institution's network to filter communication between the host server and the Cash SST;

10. Enforce pairing authentication for key Cash SST components, particularly between cash dispenser and Cash SST controller;

11. Enforce Basic Input Output System (BIOS) lock-down which include:

    (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. Ensure proper configuration and hardening of the OS and application system, which include:

    (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. Enforce secure system parameter setting, which include:

    (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. Perform scanning and removing any known malwares such as Backdoor.Padpin and Backdoor.Ploutus;

15. Enforce and monitor Cash SST end-point protection such as installing white-listing programmes. The end-point protection programme, at minimum shall ensure only authorised Cash SST system processes and libraries are installed and executed;

16. Enforce strict control procedures over installation and maintenance of Cash SST OS and application systems, which include:

(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.

17. Install close circuit cameras and transaction triggered camera at strategic locations with adequate lighting in order to ensure quality and clear CCTV 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 must ensure adequacy of physical and logical security and controls implemented on the self-service terminals, which include:

1. Enforce use of lock and key on computer terminal's central processing unit (CPU) at all times;
2. Deploy CCTV to monitor usage of self-service terminals;
3. Ensure adequate control over network security of the self-service terminals to ensure that the kiosks are secured and segregated from internal network;

4. Disable 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. Disable browser scripting, pop-ups, ActiveX, Windows shortcut;
6. Conceal Start Bar or Tray Menu;
7. Enable cache auto-deletion;
8. Disable key combinations and right-click mouse functions; and
9. Restrict use of Internet browser i.e. only to be used to access financial institution's internet website.

Appendix 3

Minimum Control Measures on Internet Banking

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

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

Question 18 How pervasive is the use of obsolete web browsers by your Internet banking users?

   (b) Deploy image or word verification authentication to enable customers to identify the financial institution's genuine website. 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) Require OTP when registering an account as a "favourite" beneficiary. A financial institution must also require a different OTP, for the first funds transfer to the favourite beneficiary;

   (d) 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 secured channels (e.g. online with 2FA or at branches); and

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

Appendix 4

Minimum Control Measures on Mobile Application and Devices

1. A financial institution must ensure digital payment, banking and insurance services involving sensitive customer information offered via mobile devices are adequately secured. This includes the following:

   (a) Ensure mobile applications run only on the supported version of operating system and enforce the application to operate on secured version of operating system 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 information used for authentication with the application server such as PIN and passwords;

   (c) Undertake proper due diligence process 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 requirements above, a financial institution must also ensure the following requirements are applied specifically for applications running on mobile devices used by the financial institution, appointed agents or intermediaries for the purpose of processing customer information:

   a) Mobile device must be adequately hardened and secured;

   b) Ensure capability to automatically wipe data stored in the mobile devices in the event the device is reported stolen or missing;

c) Physical data entry of customer's credit card information (credit card number, expiry date and CVV number) and OTP is only allowed on mobile devices owned and managed by the financial institution;

Question 19 What would be the compensating controls if an appointed agents or intermediaries' mobile device is allowed to physically key-in customer's credit card information (credit card number, expiry date and CVV number)?

d) Enforce masking of sensitive customer information when displayed on mobile devices; and

e) Limit storage of customer information for soliciting insurance businesses in mobile devices to 30 days.

3. A financial institution shall also comply with the requirements specified in paragraph 1(b) to 1(e) of Appendix 3, when providing Internet banking services over mobile devices.

Appendix 5

Minimum 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 tunnel such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec; and
   (c) Deploying staging server with adequate perimeter defenses 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 defenses 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 capability to inspect and monitor encrypted network traffic;
   (c) Web and email filtering system 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; and

(e) Solution to mitigate advanced persistent threats including zero-day and signature-less 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 Network Time Protocol (NTP) server against tampering.

Appendix 6

Positive List

Guiding Principles:

1. Does not involve introduction of new technology to the institution or industry.
2. Does not involve material change in application architecture or network design.
3. Simplified notification process does not apply to any other enhancements that are not 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), 2. Participation in approved schemes as follows: (i) Tabung Haji; (ii) Skim Simpanan Pendidikan Nasional (SSPN-i); and (iii) PayNet's products and services e.g. Real-time Retail Payments Platform (RPP), JomPAY. 3. Enable single RENTAS payment transaction initiative on Internet platform, 4. Participation in existing approved e-channel as follows: (i) Western Union; (ii) Paypal; (iii) Inter Bank Giro (IBG); and (iv) Inter Bank Fund Transfer (IBFT), 5. Increase in online transaction limit; 6. Enhancement for the following functional banking services including new add on services and features on existing platform: (i) Debit/credit card activation; (ii) Reset password; (iii) Block card including enable debit/credit card for oversea usage; (iv) Credit card pin change via Internet banking; (v) Credit card activation via SMS;	1. Enhance Transaction Authorisation Code (TAC) delivery; 2. Enhance 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 feature of Multi Factor Authentication (MFA) method; 6. Enhancement to existing features of phone banking technology.	1. System connectivity with approved schemes i.e. PayNet; 2. Financial Link external interface; 3. Installation of network devices as follows: (i) Switches; (ii) Routers; (iii) Load balancers; and (iv) Proxies. 4. Installation of security devices as follows: (i) Firewalls; (ii) Intrusion Detection Systems (IDS); and (iii) Intrusion Prevention Systems (IPS).

Guiding Principles: 1. Does not involve introduction of new technology to the institution or industry. 2. Does not involve material change in application architecture or network design. 3. Simplified notification process does not apply to any other enhancements that are not 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**
(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; and (viii) Add-on features and services from the existing Internet banking to the existing mobile application.		

Appendix 7

Attestation by the Chairman of the Board

Name of Financial Institution…. ……..……..

As Chairman of the board of directors 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 and senior management understand and are ready to assume the roles and responsibilities stated in the Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions/Guidelines on Internet Insurance (Consolidated)/Circular on Internet Takaful/Risk Management in Technology Policy Document and are also apprised of all relevant provisions in the FSA, IFSA and DFIA and other relevant legislations, 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 service 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 : ……..……..

Appendix 8

Supervisory Expectations on External Party Declaration

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

1. The assurance will 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 will 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 Declaration Report (as per Part D in Appendix 9) shall state among others scope of review, risk assessment methodology, summary of findings and remedial actions (if any).
5. The Declaration Report will confirm there is no exception noted based on the prescribed risk areas (Negative attestation).
6. Financial institution will provide the Declaration Report accompanied with the relevant documents.

Part B: Minimum control requirements to be assessed by independent External Service Provider, where applicable (to be updated over time)

1. The independent ESP assessment on 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 the following requirements shall apply:
   (a) Adequate measures to authenticate customer identity and ensure legitimate transaction authorisation by the customer;
      (i) Measures will also 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) Strong password and cryptographic implementation (recognised algorithm with reasonable key strength).

(vi) Allow data capture for payment purposes into secured mobile devices only.

(b) Adequate measures for transaction authentication that promotes non-repudiation and establish accountability:

(i) Mechanism exists to ensure proof of origin, content as well as integrity of message;

(ii) Chosen channel to deliver transaction is secured;

(iii) Mechanism exists to alert the user on certain type of transaction 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 confidentiality of information;

(vii) Use of stronger authentication for higher risk transactions; and

(viii) Timely notification to customers is sufficiently prescriptive on the nature of 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 secured mobile Operating System versions;

(ii) Application is not running on compromised devices;

(iii) Conduct penetration test to identify and rectify potential vulnerability;

(iv) Secured end-to-end communication between device to host;

(v) Sensitive information is not stored on the 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 uploading of application to application distribution platforms;

(x) Unique code is generated per transaction; and

(xi) Timely expiry of transaction code.

Appendix 9

External Party Declaration

Part A: Financial Institution	
Name of Financial Institution	
Mailing address	
Type of e-banking/Internet insurance and Internet takaful services	New / Enhancement
Description of the e-banking, Internet insurance and Internet takaful service	
Key contact personnel	
Email address	
Phone number	
Part B: Company name	
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	