TECHNOLOGY AND CYBER RISK MANAGEMENT GUIDELINE

CENTRAL BANK OF BARBADOS
May 2023

Table of Contents

Cyber Lexicon[1]

Notes:

- ***Terms defined in the lexicon are italicized when used in definitions within the lexicon.***
- ***When used in the lexicon, "entity" includes a natural person where the context requires.***

Term	Definition
Access Control	Means to ensure that access to *assets* is authorised and restricted based on business and security requirements. Source: ISO/IEC 27000:2018
Accountability	Property that ensures that the actions of an entity may be traced uniquely to that entity. Source: ISO/IEC 2382:201
Advanced Persistent Threat (APT)	A *threat actor* that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple *threat vectors*. The *advanced persistent threat*: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to execute its objectives. Source: Adapted from NIST
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. Source: ISACA Fundamentals
Authenticity	Property that an entity is what it claims to be. Source: ISO/IEC 27000:2018

[1] The Cyber Lexicon was developed by the Financial Stability Board (FSB) in an effort to foster a common understanding of relevant cyber security and cyber resilience terminology across the financial sector and other industry sectors. The terms and definitions in the lexicon were developed only for use with respect to the financial services sector and the financial institutions therein. The lexicon is not intended for use in the legal interpretation of any international arrangement or agreement or any private contract.

Term	Definition
Availability	Property of being accessible and usable on demand by an authorised entity. Source: ISO/IEC 27000:2018
Campaign	A grouping of coordinated adversarial behaviours that describes a set of malicious activities that occur over a period of time against one or more specific targets. Source: Adapted from STIX
Compromise	Violation of the security of an *information system*. Source: Adapted from ISO 21188:2018
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. Source: Adapted from ISO/IEC 27000:2018
Course of Action (CoA)	An action or actions taken to either prevent or respond to a *cyber incident*. It may describe technical, automatable responses but can also describe other actions such as employee training or policy changes. Source: Adapted from STIX
Critical (Shared) Service	An activity performed within the institution or outsourced to third parties where failure would lead to the inability to perform critical functions and, therefore, to the disruption of functions vital for the functioning of the real economy or for financial stability. Source: Adapted from the FSB Recovery and Resolution Planning for Systemically Important financial Institutions; Guidance on Identification of Critical functions and Critical Shared Services.

Term	Definition
Critical Function	An activity performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the economy and for financial stability. This can be due to the banking group or entity's size or market share, external and internal interconnectedness, complexity and cross-border activities. The function must have systemic relevance for both the third party and the financial institution. Source: Adapted from the FSB Recovery and Resolution Planning for Systemically Important financial Institutions; Guidance on Identification of Critical functions and Critical Shared Services
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and *information systems*. Source: Adapted from CPMI-IOSCO (citing NICCS)
Cyber Advisory	Notification of new trends or developments regarding a *cyber-threat* to, or *vulnerability* of, information *systems*. This notification may include analytical insights into trends, intentions, technologies or tactics used to target information *systems*. Source: Adapted from NIST
Cyber Alert	Notification that a specific *cyber incident* has occurred, or a *cyber-threat* has been directed at an organisation's *information systems*. Source: Adapted from NIST
Cyber Event	Any observable occurrence in an information system. *Cyber events* sometimes provide indication that a cyber incident is occurring. Source: Adapted from NIST (definition of "Event")

Term	Definition
Cyber Incident	A *cyber event* that: i. jeopardizes the *cyber security* of an *information system* or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. Source: Adapted from NIST (definition of "Incident")
Cyber Incident Response Plan	The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber- incident. Source: Adapted from NIST (definition of "Incident Response Plan") and NICCS
Cyber Resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to *cyber threat*s and other relevant changes in the environment and by withstanding, containing and rapidly recovering from *cyber incident*s. Source: Adapted from CERT Glossary (definition of "Operational resilience"), CPMI-IOSCO and NIST (definition of "Resilience")
Cyber Risk	The combination of the probability of *cyber incidents* occurring and their impact. Source: Adapted from CPMI-IOSCO, ISACA Fundamentals (definition of "Risk") and ISACA Full Glossary (definition of "Risk")
Cyber Security	Preservation of confidentiality, integrity and availability *of* information and/or *information systems* through the *cyber* medium. In addition, other properties, such as authenticity, *accountability, non-repudiation and reliability can also* be involved. Source: Adapted from ISO/IEC 27032:2012

Term	Definition
Cyber Threat	A circumstance with the potential to exploit one or more *vulnerabilities* that adversely affects *cyber security*. Source: Adapted from CPMI-IOSCO
Data Breach	*Compromise* of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed. Source: Adapted from ISO/IEC 27040:2015
Defence-in-Depth	Security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation. Source: Adapted from NIST and FFIEC
Denial of Service (DoS)	Prevention of authorised access to information or *information systems*; or the delaying of *information system* operations and functions, with resultant loss of *availability* to authorised users. Source: Adapted from ISO/IEC 27033-1:2015
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a *cyber-event*. Source: Adapted from NIST Framework
Distributed Denial of Service (DDoS)	A *denial of service* that is carried out using numerous sources simultaneously. Source: Adapted from NICCS
Exploit	Defined way to breach the security of information systems through *vulnerability*. Source: ISO/IEC 27039:2015

Term	Definition
Identify (function)	Develop the organisational understanding to manage *cyber risk* to *assets* and capabilities. Source: Adapted from NIST Framework
Indicators of Compromise (IoCs)	Identifying signs that a cyber-incident may have occurred or may be currently occurring. Source: Adapted from NIST (definition of "Indicator")
Identity and Access Management (IAM)	Encapsulates people, processes and technology to identify and manage the data used in an *information system* to authenticate users and grant or deny access rights to data and system resources. Source: Adapted from ISACA Full Glossary
Incident Response Team (IRT) [also known as CERT or CSIRT]	i. Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle. Source: ISO/IEC 27035-1:2016 ii. A group of individuals usually consisting of Security analysts organised to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also referred to as CERT (Computer Emergency Response Team) or CIRT Computer Incident Response Team) Source: NIST SP 800-137
Incident	i. An unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customer or user. Source: ISO/IEC 20000-1 ii. A violation or imminent threat of violation of computer security policies, acceptable use policies, guidelines or standard security practices. Source: ISACA

Term	Definition
Information Sharing	An exchange of data, information and/or knowledge that can be used to manage risks or respond to events. Source: Adapted from NICCS
Information System	Set of applications, services, information technology *assets* or other information-handling components, which includes the operating environment. Source: Adapted from ISO/IEC 27000:2018
Integrity	Property of accuracy and completeness. Source: ISO/IEC 27000:2018
IT incident	i. A single event or set of events that are not part of the ordinary delivery of IT services that causes, or may cause, an interruption to, or a reduction in, the quality and operation of that IT service. Examples include virus outbreaks, malware infiltration, system hacking, account impersonation or compromise, phishing attacks, internal sabotage or denial of service attacks.Source: Adapted from ISACA ii. Malware Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their *information systems*. Source: Adapted from ISO/IEC 27032:2012
Malware	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems. Source: Adapted from ISO/IEC 27032:2012

Term	Definition
Multi-Factor Authentication	The use of two or more of the following factors to verify a user's identity: -- knowledge factor, "something an individual knows"; -- possession factor, "something an individual has"; --biometric factor, "something that is a biological and behavioural characteristic of an individual". Source: Adapted from ISO/IEC 27040:2015 and ISO/IEC 2832- 37:2017 (definition of "biometric characteristic").
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities. Source: ISO 27000:2018
Patch Management	The systematic notification, identification, deployment, installation and *verification* of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs. Source: NIST
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an *information system*. Source: NIST
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of services and to limit or contain the impact of *cyber incidents*. Source: Adapted from NIST Framework
Recover (function)	Develop and implement the appropriate activities to maintain plans for *cyber resilience* and to restore any capabilities or services that were impaired due to a *cyber-incident*. Source: Adapted from NIST Framework

Term	Definition
Reliability	Property of consistent intended behaviour and results. Source: ISO/IEC 27000:2018
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected *cyber event*. Source: Adapted from NIST Framework
Scenario-based testing	A test that assesses a financial institution's response, resumption and recovery plans in order to strengthen operational resilience. Scenario-based tests address an appropriately broad scope of scenarios including simulation of extreme but plausible cyber-attacks, and are designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans. Scenario-based tests may use cyber threat intelligence and cyber threat modeling to the extent possible to imitate the unique characterizes of cyber threats. Examples of security incident include virus outbreak, malware infiltrations, systems hacking, account impersonation or compromise, phishing attacks, internal sabotage or denial of service attacks. Source: CPMI-IOSCO Guidance on cyber resilience for FMIs
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, store or transmits or that constitutes a violation of security policies, security procedures or acceptable user policies. Source: NIST SP 800-128
Situational Awareness	The ability to identify, process and comprehend the critical elements of information through a *cyber-threat intelligence* process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event. Source: CPMI-IOSCO

Term	Definition
Social Engineering	A general term for trying to deceive people into revealing information or performing certain actions. Source: Adapted from FFIEC
Tactics, Techniques and Procedures (TTPs)	The behaviour of a *threat actor*. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. Source: Adapted from NIST 800-150
Threat Actor	An individual, a group or an organisation believed to be operating with malicious intent. Source: Adapted from STIX
Threat Assessment	Process of formally evaluating the degree of threat to an organisation and describing the nature of the threat. Source: Adapted from NIST
Threat Intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Source: NIST 800-150
Threat-Led Penetration Testing (TLPT) [also known as Red Team Testing]	A controlled attempt to compromise the *cyber resilience* of an entity by simulating the *tactics, techniques and procedures* of real-life *threat actors*. It is based on targeted *threat intelligence* and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations. Source: G-7 Fundamental Elements

Term	Definition
Threat Vector	A path or route used by the *threat actor* to gain access to the target. Source: Adapted from ISACA Fundamentals
Traffic Light Protocol (TLP)	A set of designations used to ensure that information is shared only with the appropriate audience. It employs a pre-established color-code to indicate expected sharing boundaries to be applied by the recipient. Source: Adapted from FIRST
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. Source: ISO/IEC 27042:2015
Vulnerability	A weakness, susceptibility or flaw of an *asset* or control that can be exploited by one or more threats. Source: Adapted from CPMI-IOSCO and ISO/IEC 27000:2018
Vulnerability Assessment	Systematic examination of an information system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. Source: Adapted from NIST

Technology and Cyber Risk Management Guideline

The Technology and Cyber Risk Management Guideline ("The guideline") is general in nature, and is not intended to replace or override any legislative provisions. It should be read in conjunction with the provisions of applicable legislation as well as related guidelines issued by the Central Bank of Barbados (Bank).

1. Introduction

1.1 The advancement of information technology ("IT") has brought about rapid changes to the way businesses and operations are being conducted in the financial sector. Financial systems and networks supporting licensees' business operations have also grown in scope and complexity over the years. In most cases IT is no longer a support function for licensees, but a key enabler for business strategies including reaching out to and meeting customer needs. Licensees offering a diversity of products and services could have their financial systems operating in multiple locations and supported by different service providers.

1.2 Licensees are also faced with the challenge of keeping pace with the needs and preferences of consumers who are getting more IT-savvy and switching to internet and mobile devices for financial services, given their speed, convenience and ease of use. Increasingly, digital transformation in the financial sector, broadly characterized by the adoption of new or advanced technology, innovation, and automation, is applied to deliver improved financial services.

1.3 Licensees are deploying more advanced technology and online systems, including online payments systems, online financial services and apps with financial components, to reach their customers. In this regard, licensees should fully understand the technology and cyber risks arising from these systems. They should also put in place adequate and robust risk management systems as well as operating processes to manage these risks.

1.4 The Bank, in furtherance of its responsibilities for the regulation and supervision of licensees under the Financial Institutions Act Cap. 324A (FIA) has issued the Technology and Cyber Risk Management Guideline to provide guidance to licensees on their obligations as it relates to the management of technology and cyber risk. The Guideline sets out risk management principles and best practice standards to ensure:

a. The establishment of a sound and robust technology and cyber risk management framework;
b. The protection of customer data, transactions and systems; and
c. The consistent enhancement of system security, reliability and resilience.

1.5 This Guideline is based on the international standards and industry best practices established by a number of standard setting bodies, inclusive of, *inter alia* the National Institute of Standards and Technology (NIST), CPMI-IOSCO, ISACA, and ISO/IEC 27000.

1.6 The structure of this document is presented in Figure 1.

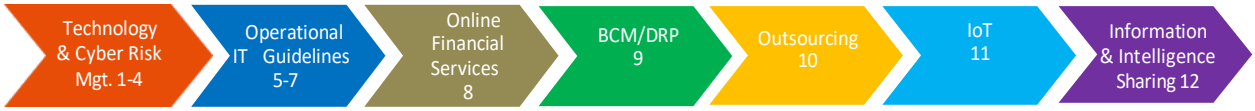

Figure 1. Structure of Guideline

2. Application and Scope

2.1 This Guideline is intended to establish a standardized approach for the management of technology and cyber risk and is applicable to all entities that are licensed under the Financial Institutions Act, CAP 324A (FIA). Licensees (including parent companies or financial holding companies for banking groups) should ensure that, at a minimum, this Guideline is also implemented in their branches and majority-owned subsidiaries abroad and, where permitted in the host country, ensure that those operations apply the higher of local and host standards. Licensees should inform the Bank if the host laws and regulations prohibit the implementation of this Guideline and take appropriate additional measures to effectively address technology and cyber risks.

2.2 The Bank recognizes that there may be differences in the approaches adopted by institutions. Licensees are therefore expected to design and implement a technology and cyber risk management framework, commensurate with the:

a. Nature and scale of the business;
b. Level of Complexity of financial services offered and supporting technologies; and
c. Degree of risk associated with each area of operation.

2.3 Notwithstanding section 2.1, where material deviations from this Guideline is contemplated, licensees must demonstrate to the Bank that the alternative measures have at least an equivalent effect of ensuring strong and effective cyber resilience. Moreover, the acceptable and proven alternative should ensure the security of all the institution's and customers' assets, relative to an agreed and established maturity level.

2.4 The Guideline contains both advisory and obligatory requirements. Advisory matters are expressed by way of the phrase "the licensee or licensees may" and licensees are permitted to implement alternative but effective measures in these circumstances. Mandatory requirements are expressed using the phrase "the licensee or licensee should".

3. Oversight of Technology and Cyber Risks by the Board and Senior Management

3.0.1 IT is a core function that facilitates the delivery of a licensees' products and services. If critical systems fail and users cannot access financial services the impact on customers would be far reaching. This would result in significant consequences to the licensee, including financial and reputational damage as well as significantly disrupting financial stability.

In view of the importance of the IT function in supporting a licensee's operations, the licensee's Board of Directors ("the Board") and Senior Management should have full oversight of technology and cyber risks and ensure that the licensee's IT function is capable of supporting its business objectives and regulatory obligations.

3.1 The Role of the Board and Senior Management

3.1.1 Licensees should utilize their existing governance structure to establish, document and oversee the implementation of an effective cyber resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimize their impact on delivering critical operations through disruption.

3.1.2 The Board should demonstrate its commitment to the oversight of technology and cyber risk management and seek to:

a. Ensure that the Board approved IT strategy is in alignment with the institution's overall business strategy.

b. Ensure that the licensee's IT strategy encompasses the management of managing technology and cyber risk and documents its cyber resilience approach considering the institution's tolerance for disruption to its critical services and functions.

c. Ensure that the licensee's policies effectively address instances where the entity's capabilities are insufficient to meet its stated tolerance for disruption.

d. Ensure to take an active role in establishing a broad understanding of the licensee's cyber resilience approach ensuring its objectives are clearly communicated to all relevant parties, including personnel, third parties and intragroup entities.

e. Ensure that the quantity and skills of the licensee's ICT staff are adequate to support its operational needs, their risk management processes on an ongoing basis and to ensure the implementation of its IT/cyber resilience strategy.

f. Ensure that Senior management set clear roles and responsibilities and establish organizational committees to ensure adequate oversight, risk ownership and accountability. For example, the three Lines of Defense.

g. Ensure that the Board comprises of member(s) with adequate IT and Cyber risk management expertise.

3.1.3 Senior Management is responsible for the implementation of the Board approved IT strategy and should ensure that a sound and robust technology risk management framework is established and maintained. Senior management should be involved in key IT decisions and:

a. Assume full responsibility for ensuring that effective internal control and risk management practices are implemented to achieve security, reliability, resiliency and recoverability.

b. Ensure that adequate technology and cyber risk awareness and management is applied throughout the licensee.

c. Inform the Board promptly of technology and cyber risk developments and incidents that may have a significant impact on the licensee, in a timely manner.

d. Ensure to monitor and evaluate existing and future trends in technology that may impact the business strategy, including monitoring of overall industry trends.

3.1.4 The Board should see to it that Section 3.1.3 is complied with, and that the corresponding risk tolerance for the licensee is understood and approved.

3.1.5 Depending on the nature, scale and complexity of its business, a licensee may establish roles for the Chief Information Security Officer (CISO). Key responsibilities that fall under this role should include *inter alia:*

CISO:

a. Implementing and overseeing the licensee's cyber security program
b. Aligning cybersecurity and business objectives
c. Reporting on cybersecurity
d. Monitoring Incident Response Activities
e. Managing Incident Response Activities
f. Managing Business continuity and disaster recovery
g. Promoting a culture of strong information security
h. Managing Information security vendor relationships
i. Utilising cybersecurity budgets effectively
j. Overseeing cybersecurity personnel within the organization
k. Ensuring cybersecurity awareness and training

3.1.6 In addition to the above, it is expected that licensee's IT and cyber policies should document additional roles and responsibilities for senior management as appropriate, to further facilitate cyber resilience. These roles may include the Chief Risk Officer (CRO), the Incident Coordinator, the Business Continuity Manager, etc.

3.1.7 Licensees should also ensure structures and programmes are in place to ensure that senior management are continually equipped to fulfill their roles and responsibilities and remain highly skilled in regard to cyber security.

3.2 IT Policies, Standards and Procedures

3.2.1 Licensees should establish IT policies, standards, and procedures to manage technology and cyber risks and safeguard information system assets[2] in the organization in line with current industry standards. The licensee's Board (or delegated committee) must remain responsible for IT policy approvals, while Senior Management or an equivalent committee assumes responsibility for the approval of IT and procedures. This facilitates the protection of licensees' information systems and information processed by such systems.

3.2.2 IT Policies and procedures reflect Board and Senior Management guidance and direction in developing controls over information systems and related resources. They should also be in alignment with business objectives, and relevant laws and regulations

3.2.3 Due to rapid changes in the IT operating and security environment, prudent implementation of policies, standards, and procedures should be reviewed, updated and approved at least annually or as needed.

3.2.4 Compliance processes should be implemented to verify that IT security standards and procedures are enforced. Follow-up processes should be implemented so that compliance deviations are appropriately ameliorated on a timely basis.

3.2.5 All licensees should establish an information security policy based on the licensee's risk assessment and mitigate the identified cyber risk threats commensurate with its risk tolerance.

3.2.6 The information security policy should be a high-level document that outlines the principles and rules to protect the confidentiality, integrity and availability of customer data and information. In defining the institution's approach to

2 Information systems assets refer to data, systems, network devices and other IT equipment.

managing information security, the policy document should contain:

a. Information security and its overall objectives and scope, as well as its alignment to business strategy and objectives.

b. A description of the main roles and responsibilities of information security management as well as staff service providers. This should also include reporting security incidents to regulators

c. A framework for establishing and implementing security measures to mitigate IT and cyber risk and should address:

- Organisation and governance.
- Logical security – procedures for logical access controls should be monitored and periodically reviewed and should include the following control elements inter alia:
  - Need to know, least privilege
  - Privileged access rights
  - Logging of user activities
  - Access management
  - Authentication methods
- Physical security – procedures for physical access should be documented and implemented to protect against unauthorised entry and environmental hazards.
- IT operations security programme – these procedures to prevent the occurrence of security issues in IT systems and its services and minimize the impact on service delivery. The measures implemented should include inter alia:
  - Identification of potential vulnerabilities
  - Implementation of secure configuration baselines of all network components
  - Implementation of network segmentation, data loss prevention and the encryption of network traffic (in accordance with data classification)
  - Implementation of protection of end points inclusive of servers, workstations, and mobile devices
  - Ensure mechanisms exist to verify the integrity of software and data

- Encryption of data at rest and in transit (in accordance with the data classification)

- Security Monitoring- this should allow the licensee to:

  - Detect anomalous activities that may impact its information security and result in the generation of appropriate alerts
  - Actively monitor technological developments to identify new vulnerabilities in hardware and software
  - Identify relevant trends in support of new or ongoing investigations
  - Ensure information security reviews and assessment
  - Ensure information security testing
  - Ensure information security training and awareness

3.3 People Selection Process

3.3.1 Careful selection of staff, vendors and contractors is crucial to minimize technology risks due to system failure, internal sabotage or fraud.

3.3.2 Licensees should implement a screening process that is comprehensive and effective, as people play an important role in managing systems and processes in an IT environment.

3.3.3 Staff, vendors and contractors, who are authorized to access a licensee's systems, should also be required to adhere to the licensee's information system security policy.

3.4 IT Security Awareness

3.4.1 A comprehensive Information security awareness training program should be established to enhance the overall IT security awareness levels within the licensee's organizational structure.

3.4.2 The training program should include information on information security policies and standards as well as each employee's individual responsibility to protect information system assets.

3.4.3 Designated employees of the licensee based on his/her role, should be made aware of the applicable laws, regulations, and guidelines pertaining to the usage, deployment and access to information security resources.

3.4.4 The information security awareness training program should be conducted and updated at least annually. This would ensure that the contents of the program remain current and relevant. The review should also take into consideration the evolving nature of technology as well as emerging risks.

3.4.5 Licensees should also ensure to take the necessary steps in order to measure and monitor the effectiveness of the security awareness training program implemented.

4. Technology and Cyber Risk Management Framework

4.0.1 A technology risk management framework should be established to manage technology and cyber risks in a systematic and consistent manner and should encompass the following attributes:

(a) Roles and responsibilities for the management of technology risks;
(b) Periodic updating of identification of information system assets and their criticality;
(c) Periodic updating of the identification and assessment of impact and likelihood of current and emerging threats, risks, and vulnerabilities;
(d) Implementation of appropriate practices and controls to mitigate risks; and
(e) Periodic update of the risk assessments to include changes in systems, environmental or operating conditions that could affect risk analysis.

4.0.2 Effective risk management practices and internal controls should be instituted to achieve data confidentiality,[3] integrity, availability, information security, reliability, resiliency and recoverability in the organization.

4.1 Information System Assets

4.1.1 Information system assets should be adequately identified, inventoried, and protected from unauthorized access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.

4.1.2 Licensees should establish clear policies on information system asset protection. Criticality of information system assets should be identified and ascertained in order to develop appropriate plans to protect them. Security and risk -based classification processes should be in place to prescribe a criticality assessment, mitigating controls, business continuity requirements, ownership, and treatment.

[3] Data confidentiality refers to the protection of sensitive or confidential information such as customer data from unauthorized access, disclosure, etc.

4.2 Risk Identification

4.2.1 Risk identification entails the determination of the threats and vulnerabilities to a licensee's IT environment which comprises the internal and external networks, hardware, software, applications, (third party) services, systems interfaces, operations and human elements throughout the supply chain.

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

4.2.3 Cybersecurity threats, such as those manifested in denial of service attacks, ransomware, internal sabotage, malware infestation, or other, could cause severe harm and disruption to the operations of a licensee with consequential losses for all parties affected. Licensees should be vigilant in identifying and monitoring such risks as it is a crucial step in the risk containment exercise.

4.3 Risk Assessment

4.3.1 Following risk identification, licensees should perform an analysis and quantification of the potential impact and consequences of these risks on their overall business and operations.

4.3.2 Licensees should analyze the impact and likelihood of the threats and vulnerabilities that could cause harm to the organization, including severe but plausible scenarios.

4.3.3 Licensees should develop a means to prioritize IT risk mitigation based on likelihood and impact assessments. In addition, licensees should assess their risk tolerance for damages and losses in the event that a given risk-related event materializes.

4.3.4 Licensees should maintain/include an IT operations security program designed to protect the confidentiality, integrity and availability of the licensee's information systems. The cybersecurity program should be based on the licensee's assessment of cyber risk and should be designed to perform the following core cybersecurity functions:

a. Identify and assess internal and external cyber risks that may threaten the security and integrity of private information stored on the licensee's information systems;

b. Use defensive infrastructure and the implementation of policies and procedures to protect the licensee's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;
c. Detect cybersecurity events;
d. Respond to identified or detected cybersecurity events to mitigate any negative effects;
e. Recover from cybersecurity events and restore normal operations and services; and
f. Fulfill applicable regulatory reporting obligations.

4.4 Risk Treatment

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

4.4.2 Risk mitigation entails a methodical approach for evaluating, prioritizing and implementing appropriate risk-reduction controls. A combination of technical, procedural, operational and functional controls would provide a rigorous mode of reducing risks and remediating identified vulnerabilities. In addition, taking insurance cover for various insurable risks, including recovery and restitution costs should be considered.

4.4.3 As it may not be practical to address all known risks simultaneously or in the same timeframe, licensees should give priority to threat and vulnerability pairings that could cause significant harm or impact to a licensee's operations.

4.4.4 It is imperative that licensees are able to manage and control risks in a manner that will maintain their financial and operational viability and stability. When deciding on the adoption of risk controls and security measures, licensees should balance the impact to all stakeholders against the benefits to be derived.

4.4.5 Licensees should refrain from implementing and running a system where the threats to the safety and soundness of their core and critical IT services are insurmountable and the risks cannot be adequately controlled.

4.5 Risk Monitoring and Reporting

4.5.1 Licensees should maintain a risk register which facilitates the monitoring and reporting of risks. Risks of the highest severity should be accorded top priority and monitored closely with regular reporting on the actions that have been

taken to mitigate them. Licensees should update the risk register periodically, and institute a monitoring and review process for continuous assessment and treatment of risks.

4.5.2 To facilitate risk reporting to management, licensees should develop IT risk metrics to highlight systems, processes or infrastructure that have the highest risk exposure. An overall cyber risk profile of the organization should also be provided to the Board and Senior Management. In determining the IT risk metrics, licensees should consider risk events, regulatory requirements and audit observations.

4.5.3 Risk parameters may shift as the IT environment and delivery channels change. Thus, licensees should review and update the risk processes accordingly, and conduct, at a minimum, an annual evaluation of risk-control methods that includes an assessment of the adequacy and effectiveness of IT controls and risk management processes. The frequency of the evaluations should be determined by changes to the licensee's environment, business circumstances, legal conditions, or the IT environment.

4.5.4 Management of the IT function should review and update its IT risk control and mitigation approach, considering the changing cyber landscape and variations in the licensee's risk profile.

5. Operational IT Risk Guidelines

5.0.1 Many systems fail due to poor system design and implementation, as well as inadequate testing. Licensees should identify system deficiencies and defects at the system design, development and testing phases. Moreover, Licensees should establish a foundation for IT maturity and IT project management where the focus specifically lies on security requirements, testing of systems and end user risks to solidify the IT landscape.

5.0.2 Ongoing attention should be given to the sufficiency of the IT security measures in place and risk management throughout the project life cycle.

5.1 IT Project Management

5.1.1 The management of all projects initiated within licensee should be in alignment with the Board approved IT strategy and conducted using the standard project management approach which would include phases such as initiation, planning, control and execution, closure and post implementation review.

5.1.2 In establishing a project management framework, licensees should ensure *inter alia*, that:

a. Roles and responsibilities are defined which facilitates governance and management review, decision making and delivery management activities.
b. The nature and scope of the project is defined to confirm and develop a common understanding of project scope among stakeholders.
c. Tasks and processes for developing or acquiring new systems include project risk assessment and classification and critical success factors are defined for each project phase.
d. The approach to project quality and implementation is well defined and a record is maintained of any risks faced by project management.
e. Project performance is measured against project performance criteria.
f. Project resources are managed effectively.

5.1.3 Licensees should also establish a steering committee for large or complex projects, consisting of business owners, the development team and other stakeholders to provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable. The steering committee should have a clear communication line with Senior Management.

5.1.4 Licensees should clearly document project plans for all IT projects. In the project plans, licensees should clearly set out the deliverables to be realized at each phase of the project as well as milestones to be reached.

5.1.5 Licensees should ensure that functional, performance and security requirements, business cases, cost benefit analysis, systems design, technical specifications and test plans are approved by the relevant business and IT management.

5.1.6 Licensees should establish management oversight of the project to ensure that milestones are reached, and deliverables are realized in a timely manner. Licensees should escalate issues or problems which could not be resolved at the project committee level to Senior Management for attention and intervention.

5.2 System Security Requirements and Testing

5.2.1 Licensees should clearly specify security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling in the early phase of system development or acquisition.

5.2.2 A methodology for system testing[4] should be established. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

5.2.3 Licensees should ensure that appropriate testing is performed based on the risk of the system changes being deployed. This includes full regression testing for major systems. Users whose systems and operations are affected by the system changes should review and sign off on the outcome of the tests.

5.2.4 Licensees should conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces. In the event that a licensee deviates from this decision, they should document exceptions properly and have them available to the Bank upon request. In case no prior penetration testing is possible, penetration testing should be performed within the first six (6) months after implementation, explained and documented. Licensees unable to commit to this timeframe must write to the Bank to advise of any challenges experienced accompanied with an action plan. Licensees should also perform continuous vulnerability scanning of external and internal network components that support the changed and current system landscape.

5.3 End User Development

5.3.1 There are common business application tools and software which allow business users to develop simple applications to automate their operations, perform data analysis and generate reports for the licensee and customers. Licensees should perform an assessment to ascertain the importance of these applications to the business.

5.3.2 Recovery measures, user access and data protection controls, at a minimum, should be implemented for such applications.

5.3.3 Licensees should review and test, end user developed program codes, scripts and macros based on the risk assessment conducted. This should be done before these applications are used to verify their integrity and reliability.

5.4 IT Audit

5.4.1 As technology risks evolve with the growing complexity of the IT environment, there is an increasing need for licensees to develop effective internal control systems to manage technology risks.

[4] System testing is broadly defined to include unit, modular, integration, system and user acceptance testing

5.4.2 IT audit provides the Board and Senior Management with an independent and objective assessment of the effectiveness of controls that are applied within the IT environment to manage technology and cyber risks.

5.4.3 Licensees should establish an organizational structure and reporting lines for IT audit in a way that preserves the independence and objectivity of the IT audit function.

5.5 Audit Planning and Remediation Tracking

5.5.1 Licensees should ensure that the scope of IT audit is comprehensive and includes all critical IT operations. An IT audit plan, comprising auditable IT areas for the coming year, should be developed. The IT audit plan should be approved annually by Senior Management and the Board.

5.5.2 Licensees should establish an audit cycle that determines the frequency of IT audits. The audit frequency should be commensurate with the criticality and risk of the IT system or process.

5.5.3 The audit should be performed independently by an Internal audit function, or an external auditor, employing a risk-based approach, with the capacity to review and provide objective assurance of compliance with the licensee's information security policies and procedures as well as regulatory guidance.

5.5.4 The auditors should be sufficiently knowledgeable and possess the requisite skills and expertise in IT and cyber risk controls in order to conduct the audit efficiently and effectively.

5.5.5 A formal follow-up process including provisions or the timely verification and remediation of critical IT and cybersecurity audit findings should be established.

6. IT Service Management

6.0.1 A robust IT service management framework is essential for supporting IT systems, services and operations, managing changes, incidents and problems as well as ensuring the stability of the production IT environment.

6.0.2 The framework should comprise the governance structure, processes and procedures for change management, software release management, incident and problem management as well as capacity management, program migration and managing of (privileged) user access onto the IT landscape.

6.1 Change Management

6.1.1 Licensees should establish a change management process to ensure that changes to production systems are logged, assessed, prioritized, approved, scheduled, implemented, and reviewed in a controlled manner.

6.1.2 A tracking and reporting system should be maintained to document rejected changes and communicate the status of approved, in-process and completed changes.

6.1.3 All change requests should be evaluated to determine the impact on business processes, IT services, and assessed to determine any adverse effect on the operational environment and any introduction of unacceptable risk.

6.1.4 The change management process should include automated system and security configurations, patches for hardware devices and software updates.

6.1.5 Prior to deploying changes to the production environment, licensees should perform a risk and impact analysis of the change request in relation to existing infrastructure, network, up-stream and downstream systems. Licensees should also determine if the introduced change would spawn security implications or software compatibility problems to affected systems or applications.

6.1.6 Licensees should adequately test the impending change and ensure that it is accepted by users prior to the migration of the changed modules to the production system. Licensees should develop and document appropriate test plans for the impending change. Licensees should also obtain test results with user sign-offs prior to the migration.

6.1.7 All changes to the production environment should be approved by personnel delegated with the authority to approve change requests.

6.1.8 To minimize risks associated with changes, licensees should perform backups of affected systems or applications prior to the change. Licensees should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment. Licensees should establish alternative recovery options to address situations where a change does not allow a licensee to revert to a prior status.

6.1.9 Audit and security logs are useful information which facilitates investigations and troubleshooting. Licensees should ensure that the logging facility is enabled to record activities that are performed during the migration process.

6.2 Program Migration

Program migration involves the movement of software codes and scripts from the development environment to test and production environments. Unauthorized and malicious codes which are injected during the migration process could compromise data, systems, and processes in the production environment.

6.2.1 Licensees should separate physical or logical environments for systems development, testing (e.g. user and system acceptance testing), staging, and production.

6.2.2 Licensees should closely monitor vendor and developers' access to all their environments.

6.2.3 Where controls in the non-production environment are different or less stringent from those in the production environment, licensees should perform a risk assessment and ensure that sufficient preventive and detective controls have been implemented before connecting a non-production environment to the internet.

6.2.4 Segregation of duties should be enforced where feasible so that no single individual has the ability to develop, compile, and move object codes from one environment to another. In cases where segregation of duties is not completely possible, licensees should document and explain this process as well as present a suitable alternative.

6.2.5 After a change has been successfully implemented in the production environment, the change should also be replicated and migrated to disaster recovery systems or applications for consistency.

6.3 User Access Management

6.3.1 Licensees should only grant user access to IT systems and networks on a need-to-use basis and within the period when the access is required. Licensees should ensure that the resource owner duly authorizes and approves all requests to access IT resources.

6.3.2 Employees of vendors or service providers, who are given authorized access to Licensees critical systems and other computer resources, pose similar risks as internal staff. Licensees should subject these external employees to close supervision, monitoring and access restrictions similar to those expected of its own staff.

6.3.3 For accountability and identification of unauthorized access, licensees should ensure that records of user access are uniquely identified and logged for audit and review purposes.

6.3.4 Licensees should perform regular reviews of user access privileges to verify that privileges are granted appropriately and according to the 'least privilege' principle. The process may facilitate the identification of dormant and redundant accounts as well as detection of wrongly provisioned access.

6.3.5 Passwords represent the first line of defense, and if not implemented appropriately, they can be the weakest link in the organization. Thus, licensees should enforce strong password controls over users' access to applications and systems. Password controls should include a change of password upon first logon, minimum password length and history, password complexity as well as maximum validity period.

6.3.6 Licensees should ensure that no one has concurrent access to both production systems and backup systems, particularly data files and computer facilities. Licensees should also ensure that any person who needs to access backup files or system recovery resources is duly authorized for a specific reason and a specified time only.

6.4 Privileged Access Management

6.4.1 Information security ultimately relies on trusting a small group of skilled staff, who should be subject to proper checks and balances. Their duties and access to systems resources should be placed under close scrutiny. Licensees should apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions, considering insider threat.

6.4.2 Licensees should adopt the following controls and security practices:

a. Implement strong authentication mechanisms such as two-factor authentication where possible for privileged users;
b. Institute strong controls over remote access by privileged users;
c. Restrict the number of privileged users;
d. Grant privileged access on a "need-to-have" basis;
e. Maintain audit logging of system activities performed by privileged users;
f. Disallow privileged users from accessing systems logs in which their activities are being captured;
g. Review privileged users' activities on a timely basis;
h. Prohibit sharing of privileged accounts;

i. Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and
j. Protect backup data from unauthorized access.

6.5 Remote Access Management

6.5.1 Remote access allows users to connect to the licensee's internal network via an external network to access the licensee's data and systems, such as emails and business applications. Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users that have remote access. This should safeguard against unauthorized access to the licensee's IT environment.

6.5.2 Licensees should only allow remote access to the its information assets from devices that have been secured, hardened and are fully patched according to their endpoint security standards.

6.5.3 Remote access infrastructure should be thoroughly tested for vulnerabilities. If cloud infrastructure is used, review of existing controls, security assessment and security testing should also be conducted to make sure the controls work effectively.

6.5.4 User IT Security awareness training remains crucial for users that are new to the technology usage, to minimize exposure to phishing and social engineering.

6.5.5 Functions dealing with critical system processes and data are normally not allowed through remote access. If the situation so requires, existing controls will need to be re- evaluated, or activated when required.

6.6 Incident Management

6.6.1 The occurrence of an IT incident may result in the disruption, malfunction or error on a licensee's server, network or end point which can impact its operations and service delivery. It can also lead to other external systems becoming affected. Licensees should appropriately manage such incidents to understand the root cause and appropriate preventative measures to reduce prolonged disruption of IT services or further aggravation.

6.6.2 Licensees should establish an incident management plan with the objective of restoring normal IT service as quickly as possible following the incident, and with minimal impact to the licensee's business operations. Licensees should also establish the roles and responsibilities of staff involved in the incident management process, which includes recording, analyzing, remediating, and monitoring incidents.

6.6.3 It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, licensees may delegate the function of determining and assigning incident severity levels to a centralized technical helpdesk function. Licensees should train helpdesk staff to discern incidents of high severity level. In addition, criteria used for assessing severity levels of incidents should be established and documented.

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

6.6.5 A licensee's internal communication plans should also address security-related customer complaints to ensure that:

a. Incidents with a potentially high unfavorable impact on critical IT systems and services are reported to the relevant senior officer.
b. In the event of a major incident, senior management is informed periodically in order to effectively implement additional controls as required.

6.6.6 Licensees should form a computer emergency response team (CERT), comprising staff with the necessary technical and operational skills to handle major incidents.

6.6.7 In some situations, major incidents (in terms of cost, image, number of clients affected) may develop into a crisis. Senior Management should be kept apprised of the development of these incidents in real time so that the decision to activate the disaster recovery plan can be made on a timely basis. An incident should be classified within the first twenty-four (24) hours of its detection. An incident is classified as major if it satisfies the requisite criteria in the Classification Matrix found in the Appendix in the M-CIRT instructions. Licensees should complete the stage 1 section of the template referred to as the Initial report and submit it to the Bank within (4) hours after an incident is classified as major.

6.6.8 Notwithstanding the above, the Bank should be contacted promptly pending the submission of the report template, as applicable:

a. Where a matter is classified as major within twenty-four (24) hours; or
b. Where a matter reaches the media or social platforms.

6.6.9 The maintenance of customer confidence throughout a crisis or an emergency situation is of great importance to the reputation, operation and soundness of licensees. Therefore, licensees should include in their incident response procedures a predetermined action plan to keep customers informed of any major incidents where their data has potentially been compromised and/or funds withdrawn without their permission. They should also assess the effectiveness of the mode of communication to the general public, customers staff and other relevant stakeholders.

6.6.10 Licensees should keep customers informed of any major incident or data breach, where their data has potentially been compromised. They should also assess the effectiveness of the mode of communication, including informing the general public, where necessary.

6.6.11 Included in the incident response plan, licensees should establish an external communication action plan for critical business functions and processes to facilitate:

a. Effective collaboration with relevant stakeholders in order to respond to and recover from an incident.
b. Information sharing with external parties (i.e. other financial sector participants, supervisory authorities and law enforcement authorities) as appropriate, enabling continuous learning as a collective, resulting in actionable and strategic intelligence.

6.6.12 As incidents may stem from numerous factors, licensees should perform a root cause and impact analysis for major incidents which result in disruption of critical IT services. Licensees should take remediation actions to prevent the recurrence of similar incidents and security breaches.

6.6.13 Licensees should include in their internal operational incident report an executive summary of the major incident, an analysis of root cause which triggered the event, its impact as well as measures taken to address the root cause and consequences of the event.

6.6.14 Licensees should adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution.

6.6.15 Cybersecurity events that have a reasonable likelihood of materially harming any part of the normal operation(s) of the licensee and classified as major[5], should also be reported via the Major Cyber Incident Reporting Template (M-

[5] Refer to the classification matrix in the M-CIRT Instructions.

CIRT)[6] to the Bank. A major incident is one classified as either high or critical. Annually each licensee should revise their Cybersecurity program where it has identified areas, systems or processes that require material improvement, updating or redesign. Licensees should document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Bank.

6.6.16 In order to effectively manage incidents, licensees need to have means to prioritize them, incidents may be prioritized by an Impact vs. Urgency matrix.

6.6.17 Impact is the effect incident has on a business, and Urgency basically defines time business (or customer) is ready to wait for resolution.

6.6.18 According to Information Technology Infrastructure Library (ITIL), Priority should be a product of the Impact/Urgency matrix. It is customary that Priority has four levels, and is marked with the numbers 1-4, where "1" is the highest and "4" is the lowest priority. It can also be marked by letters ABCD, with A being the highest priority. Impact can be defined as the severity of the incident, for example, how much downtime or how many end users are affected, while urgency is how quickly the incident needs to be resolved. The most commonly used priority matrix is reflected in Figure 2:

Impact	Urgency	Priority
High	High	(1) Critical
High	Medium	(2) High
High	Low	(3) Moderate
Medium	High	(2) High
Medium	Medium	(3) Moderate
Medium	Low	(4) Low
Low	High	(3) Moderate
Low	Medium	(4) Low
Low	Low	(4) Low

Figure 2: Incident Management Prioritization Matrix

6.6.19 In theory for example, a major incident is a highest-impact, highest-urgency incident. It affects a large number of users, depriving the business of one or more crucial services. Licensees can define what "High", "Medium" and "Low" Impact is from the Incident Classification Matrix, and inform the Bank of any additional incidents added urgency can be defined as the four (4) levels of

[6] Refer to the Cyber Incident Reporting Template and accompanying Instructions.

downtime also depicted in the Classification Matrix.

6.6.20 Licensees should continuously identify and address any gaps in their cyber incident response capabilities.

6.6.21 The cyber incident response plan should include plausible scenarios. In addition, table top exercises should also be conducted periodically.

6.6.22 The licensee should implement and maintain management information systems, appropriate to the scale, nature and complexity of its operations, to enable efficient cyber incident analysis and reporting.

6.7 Problem Management

6.7.1 The licensee should establish problem management processes and procedures to determine and resolve the root cause of incidents to prevent the recurrence of similar incidents.

6.7.2 The licensee should record incidents including the lessons learnt to facilitate the diagnosis and resolution of future incidents with similar characteristics.

6.7.3 A trend analysis of past incidents should be performed by the licensee to identify commonalities and patterns in the incidents, and verify if the root causes to the problems had been properly identified and resolved. The licensees should also use the analysis to determine if further measures are necessary.

7. Operational Infrastructure Security Management

7.0.1 The IT landscape is vulnerable to various forms of cyber-attacks[7] and the frequency and malignancy of attacks are increasing. It is imperative that Licensees implement security solutions at the data, application, database, operating systems and network layers to adequately address and contain these threats.

7.0.2 Appropriate technological measures should be implemented to protect sensitive or confidential information such as customer's personal, account and transaction data which are stored and processed in systems. Customers should be properly authenticated before access to online transaction functions and sensitive personal or account information is permitted. Sensitive customer information including login credentials, passwords and personal identification numbers (PINs), multi-factor

[7] Cyber-attacks include phishing, denial of service attacks, spamming, sniffing, spoofing, hacking, keylogging, phishing, middleman interception, and other malware attacks from mutating virus and worms

authentication (MFA) mechanisms should be secured against exploits such as ATM skimming, hacking, phishing and malware.

7.0.3 Special care must be taken to manage and monitor the use of system and service accounts for suspicious or unauthorized activities, to protect all components if a virtualization solution is used, including the hypervisor, virtual images and snapshots, and to vet and strongly secure any Application Programming Interfaces (APIs)[8] and Keys from introduction till retirement.

7.1 Data Loss Prevention

7.1.1 Internal sabotage, clandestine espionage or furtive attacks by trusted staff, contractors and vendors are potentially among the most serious risks that Licensees could face in an increasingly complex and dynamic IT environment. Current and past staff, contractors, vendors and those who have knowledge of the inner workings of the institution's systems, operations and internal controls, have a significant advantage over external attackers. A successful attack not only jeopardizes customer confidence in the licensee's internal control systems and processes but also causes real financial loss when proprietary information is divulged. Licensees should identify important data and adopt adequate measures to detect and prevent unauthorized access, copying or transmission of confidential information.

7.1.2 Licensees should develop a comprehensive data loss prevention strategy to protect sensitive or confidential information, taking into consideration the following:

a) Data at endpoint - Data which resides in notebooks, personal computers, portable storage devices and mobile devices;

b) Data in motion - Data that traverses a network or that is transported between sites; and

c) Data at rest - Data in computer storage which includes files stored on servers, databases, backup media and storage platforms.

7.1.3 To achieve security of data at endpoints, Licensees should implement appropriate measures to address risks of data theft, data loss and data leakage from endpoint devices, customer service locations, and call centers. Licensees should protect confidential information stored in all types of endpoint devices with strong encryption and access controls.

7.1.4 Licensees should not divulge confidential information through social media sites.

[8] API's are access points that allow user and program interaction with an application.

7.1.5 For the purpose of exchanging confidential information with external parties, licensees should take utmost care to preserve the confidentiality and integrity of information. For this purpose, licensees should at all times take appropriate measures including sending information through encrypted channels (e.g. via encrypted mail protocol) or encrypting the email and the contents using strong encryption with adequate key length that meets its security objectives and requirements. Licensees should send the encryption key via a separate transmission channel to the intended recipients. Alternatively, Licensees may choose other secure means to exchange confidential information with its intended recipients.

7.1.6 Confidential information stored on IT systems, servers, and databases should be encrypted and protected through strong access controls, bearing in mind the principle of "least privilege"[9].

7.1.7 Licensees should assess various methods in which data could be securely removed from the storage media and implement measures to prevent the loss of confidential information through the disposal of IT systems. In determining the appropriate media sanitization method to use, licensees should take into consideration security requirements of the data residing on the media.

7.2 Technology Refresh Management

7.2.1 To facilitate the tracking of IT resources, Licensees should maintain an up-to-date inventory of software and hardware components used in the production and disaster recovery environments which includes all relevant associated warranty and other support contracts related to the software and hardware components.

7.2.2 Licensees should actively manage their IT systems and software so that outdated and unsupported systems which significantly increase its exposure to technology risks are replaced on a timely basis. Licensees should pay close attention to the product's end-of- support ("EOS") date as it is common for vendors to cease the provision of patches, including those relating to security vulnerabilities that are uncovered after the product's EOS date.

7.2.3 Licensees should establish a technology refresh plan to ensure that systems and software are replaced in a timely manner. Licensees should conduct a risk assessment for systems approaching EOS dates to assess the risks of continued usage and establish effective risk mitigation controls where necessary.

[9] Least privilege is defined as assigned privileges on a "need-to-have" basis

7.3 Networks and Security Configuration Management

7.3.1 Licensees should configure IT systems and devices with security settings that are consistent with the expected level of protection and minimize their exposure to cyber threats. Licensees should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment.

7.3.2 Licensees should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly, and non-compliances is detected and raised for investigation.

7.3.3 Licensees should deploy anti-malware software to servers, if applicable, and workstations. Licensees should ensure that the anti-malware software updates its definition files daily and schedule automatic anti-malware scanning on servers and workstations on a daily basis.

7.3.4 Licensees should install network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical junctures of their IT infrastructure to protect the network perimeters. Additional security mechanisms should be deployed to minimize the risk of lateral movement during a cyber-attack and insider threat behavior. Licensees should deploy firewalls, or other similar measures, within internal networks to minimize the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network. On an annual basis, licensees should also review rules on network security devices to determine that such rules are still appropriate and relevant.

7.3.5 Licensees deploying Wireless Local Area Networks (WLAN) within the organization should be aware of the risks associated herewith. Measures, such as secure communication protocols for transmissions between access points and wireless clients, should be implemented to secure the corporate network from unauthorized access.

7.3.6 A review of the licensee's network architecture, including the network security design, as well as system and network interconnections, should be conducted on a periodic basis to identify potential cybersecurity vulnerabilities.

7.4 Vulnerability Assessment and Penetration Testing (VAPT)

7.4.1 Vulnerability Assessment (VA) is the process of identifying, assessing and discovering security vulnerabilities in a system. Licensees should conduct VAs at least annually to detect security vulnerabilities in the IT environment and

should be commensurate with the criticality of the IT system and the technology risk to which it is exposed.

7.4.2 Licensees should deploy a combination of automated tools and manual techniques to perform a comprehensive VA of both operating systems and software applications. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting.

7.4.3 Licensees should establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed.

7.4.4 Licensees should carry out penetration tests in order to conduct an in-depth evaluation of the cybersecurity posture of the system through simulations of actual attacks on the system. Licensees may conduct penetration tests on internet-facing systems at least annually, or whenever these systems undergo major changes or updates. Full scope penetration tests should be conducted at least once every two years as deemed applicable.

7.4.5 Licensees may have VAPT conducted by independent testers with sufficient knowledge, skills and expertise in testing information security measures and who are not involved in the development of the information security measures.

7.4.6 Another type of penetration testing known as Threat-Level Penetration Testing (TLPT), may also be conducted by licensees. The purpose of TLPT is to assess and provide insights on entities resilience capabilities against a real world simulated cyber incident. The scope and risk management of the simulation would be proportionate to the type size, complexity, structure and risk profile of the licensee.

7.4.7 Licensees may also conduct scenario-based testing which is designed to benchmark the performance of cyber security controls against specific adversarial tactics and behaviours. These exercises can be market-driven or regulator driven and can result in a more resilient financial sector.

7.5 Patch Management

7.5.1 Licensees should establish and ensure that the patch management procedures include the identification, categorization, and prioritization of security patches. To implement security patches in a timely manner, licensees should establish the implementation timeframe for each category of security patches.

7.5.2 The application of patches, if not carried out appropriately, could potentially impact other peripheral systems. As such, licensees should perform adequate testing of security patches before deployment into the production environment.

7.6 Security Monitoring and Detection

7.6.1 Security monitoring is an important function within the IT environment to detect malicious attacks on IT systems. To facilitate prompt detection of unauthorized or malicious activities by internal and external parties, licensees should establish appropriate security monitoring systems and processes.

7.6.2 Licensees should implement network surveillance and security monitoring procedures with the use of network security devices, such as intrusion detection and prevention systems, to protect their institution against network intrusion attacks as well as to provide alerts when an intrusion occurs.

7.6.3 Licensees should implement security monitoring tools which enable the detection of changes to critical IT resources such as databases, system or data files and programs, to facilitate the identification of unauthorized changes. Licensees should include capacity management to support business functions, and ensure that indicators such as performance, capacity, and utilization are monitored and reviewed.

7.6.4 Licensees should perform real-time monitoring of security events for critical systems and applications, to facilitate the prompt detection of malicious activities on these systems and applications.

7.6.5 Licensees should review security logs of systems, applications, and network devices for anomalies at least monthly. Licensees should closely supervise staff with elevated system access entitlements and have all their system activities logged and reviewed at least semi-annually, as they have the knowledge and resources to circumvent system controls and security procedures.

7.6.6 To enhance the effectiveness of security monitoring, the licensee should consider applying user behavioral analytics. User behavioral analytics could include the use of machine learning algorithms in real time to analyze system logs, establish a baseline of normal user activities and identify suspicious or anomalous behaviors.

7.6.7 Licensees should adequately protect and retain system logs to facilitate any future investigation. When determining the log retention period, licensees should consider statutory requirements for document retention and protection.

8. Online Financial Services[10]

8.0.1 Whilst the internet presents opportunities for licensees to reach new markets and expand its range of products and services, being an open network, it also exposes the institution to cyber-attacks that are more sophisticated and dynamic compared to those attacking closed networks and proprietary delivery channels. Licensees should be cognizant of these risks that are facilitated as a result of offering financial services via the internet platform.

8.0.2 Licensees should clearly identify risks associated with the types of services being offered in the risk management process. Licensees are expected to also formulate security controls, system availability and recovery capabilities, which are commensurate with the level of risk exposure, for all internet operations.

8.1 Online Systems Security

8.1.1 Licensees should devise a security strategy and put in place measures to ensure the confidentiality, integrity and availability of its data and systems.

8.1.2 Licensees should provide their customers and users of their internet services the assurance that online login access and transactions performed over the internet on their websites are adequately protected and authenticated.

8.1.3 The Bank expects licensees to properly evaluate the security requirements associated with their internet systems and adopt encryption algorithms, with due regard of the international standards in this area (e.g. ISO 18033-3 encryption algorithms).

8.1.4 Licensees should ensure that information processed, stored or transmitted between itself and its customers is accurate, reliable and complete. With internet connection to internal networks, financial systems and devices may now be potentially accessed by anyone from anywhere at any time. Licensees should implement physical and logical access security to allow only authorized personnel to access its systems. Licensees should also implement

[10] Online financial services refer to the provision of banking, trading, insurance or other financial services and products via electronic delivery channels based on computer networks or internet technologies, including fixed line, cellular or wireless networks, web-based applications and mobile devices

appropriate processing and transmission controls to protect the integrity of systems and data.

8.1.5 Licensees should implement monitoring or surveillance systems so that it is alerted to any abnormal system activities[11], transmission errors or unusual online transactions. Licensees should establish a follow-up process to verify that these issues or errors are adequately addressed.

8.1.6 Licensees should maintain high resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment). Licensees should put in place measures to plan and track capacity utilization as well as guard against online attacks. These online attacks may include denial-of-service attacks (DoS attack) and distributed denial-of-service attack (DDoS attack).

8.1.7 Licensees should implement multi-factor authentication[12] (MFA) at login for all types of online financial systems[13] and transaction-signing for authorizing transactions. The primary objectives of multi-factor authentication and transaction-signing are to secure the customer authentication process and to protect the integrity of customer account data and transaction details as well as to enhance confidence in online systems by combating cyber-attacks targeted at licensees and their customers.

8.1.8 Licensees should also take appropriate measures to minimize exposure to other forms of cyber-attacks such as the middleman attack which is more commonly known as a man-in-the-middle attack[14] (MITMA), man-in-the-browser attack or man-in-the-application attack.

8.1.9 As more customers log onto licensees' websites to access their accounts and conduct a wide range of financial transactions and services for personal and business purposes, licensees should put in place measures to protect customers who use online payment systems. In addition, licensees should educate its customers on security measures that are put in place to protect their customers in an online environment.

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

[12] Multifactor-factor authentication for system login can be based on any two of the factors, i.e. What you know (e.g. PIN), what you have (e.g. OTP token) and who you are (e.g. Biometrics).

[13] Online financial services refer to the provision of banking, trading, insurance or other financial services and products via electronic delivery channels based on computer networks or internet technologies, including fixed line, cellular or wireless networks, web-based applications and mobile devices

[14] In a man-in-the-middle attack, an interloper is able to read, insert and modify messages between two communicating parties without either one knowing that the link between them has been compromised. Possible attack points for MITMA could be customer computers, internal networks, information service providers, web servers or anywhere in the internet along the path between the customer and the FI's server

8.2 Mobile Online Services and Payments Security

8.2.1 Mobile Online Services refers to the provision of financial services via mobile devices such as mobile phones or tablets. Customers may choose to access these financial services via web browsers on mobile phones or self-developed applications on mobile platforms. Mobile payment refers to the use of mobile devices to make payments. These payments may be made using various technologies such as near-field communication (NFC).

8.2.2 Mobile online services and payments are extensions of the online financial services and payments services which are offered by licensees and accessible from the internet via computers or laptops. Licensees should implement security measures which are similar to those of online financial and payment systems on the mobile online services and payment systems. Licensees should conduct a risk assessment to identify possible fraud scenarios and put in place appropriate measures to counteract payment fraud via mobile devices.

8.2.3 As mobile devices are susceptible to theft and loss, licensees should ensure that there is adequate protection of sensitive or confidential information used for mobile online services and payments. Licensees should have sensitive or confidential information encrypted to ensure the confidentiality and integrity of this information in storage and transmission. Licensees should perform the processing of sensitive or confidential information in a secure environment.

8.2.4 Licensees should educate their customers on security measures to protect their own mobile devices from viruses and other errant software which cause malicious damage and have harmful consequences. This can be facilitated via a combination of workshops and various social media notices.

8.3 Payment Card Security (ATMs, Credit and Debit Cards)

8.3.1 Payment cards[15] allow cardholders the flexibility to make purchases from any location. Cardholders may choose to make purchases by physically presenting these cards for payments at the merchant or they could choose to purchase their items over the internet, or over the telephone. Payment cards also provide cardholders with the convenience of withdrawing cash at automated teller machines (ATMs) or conducting payments at point of sales (POS) located at merchants.

8.3.2 Payment cards exist in many forms; with magnetic stripe cards posing the highest risk exposure. Licensees that issue cards should follow international

[15] For the purpose of this document, "payment cards" refer to ATM, credit, charge and debit cards

standards of migrating away from magnetic stripe card types to other, safer, methods (e.g. EMV chip supported card transactions).

8.3.3 Types of payment card fraud include counterfeit, lost/stolen, card-not received[16] ("CNR") and card-not-present[17] ("CNP") fraud. Licensees should therefore monitor payments patterns for insider threat.

8.4 Payment Card Fraud

8.4.1 Licensees that provide payment card services should implement adequate safeguards to protect sensitive payment card data. Licensees should ensure that sensitive payment card data is (PCI compliant) encrypted to ensure the confidentiality and integrity of these data in storage and transmission, and the processing of sensitive or confidential information is done in a secure environment.

8.4.2 Licensees should deploy secure methods to store sensitive payment card data. Licensees should also implement strong card authentication methods such as dynamic data authentication ("DDA") or combined data authentication ("CDA") methods for online and offline card transactions. For interoperability reasons, where transactions could only be affected by using information from the magnetic stripe on a card, Licensees should ensure that robust controls are implemented to manage these transactions.

8.4.3 The licensee's card issuer, and not a third-party payment processing service provider, should perform the authentication of customers' sensitive static information, such as PINs or passwords. Licensees should perform regular security reviews of the infrastructure and processes being used by their service providers and merchants.

8.4.4 Licensees should ensure that security controls are implemented at payment card systems and networks.

8.4.5 To enhance card payment security, licensees should promptly notify cardholders via transaction alerts when withdrawals/charges exceeding customer-defined thresholds are made on the customers' payment cards. Licensees should implement robust fraud detection systems with behavioral scoring or equivalent; and correlation capabilities to identify and curb fraudulent activities. Licensees should set out risk management parameters according to risks posed by cardholders, the nature of transactions or other risk factors to enhance fraud detection capabilities.

[16] Card-not-received fraud refers to fraud cases where cardholders do not receive cards dispatched by the issuing banks and subsequently, these cards are used to make fraudulent transactions.

[17] Card-not-present fraud involves the use of stolen or compromised card details to make purchases over the internet, phone or mail order

8.4.6 Licensees should follow up on transactions exhibiting behavior which deviates significantly from a cardholder's usual card usage patterns. Licensees should investigate these transactions and obtain the cardholder's authorization prior to completing the transaction.

8.5 ATMs and Payment Kiosks Security

8.5.1 The presence of ATMs and payment kiosks have provided cardholders with the convenience of withdrawing cash as well as making payments to billing organizations. However, these systems are targets where card skimming attacks are perpetrated.

(a) To secure consumer confidence in using these systems, licensees should put in place the following measures to counteract fraudsters' attacks on ATMs and payment kiosks: Install anti-skimming solutions on these machines and kiosks to detect the presence of foreign devices placed over or near a card entry slot;
(b) Install detection mechanisms and send alerts to appropriate staff at licensee for follow- up response and action;
(c) Implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission;
(d) Implement appropriate measures to prevent shoulder surfing of customers' PINs; and
(e) Conduct video surveillance of activities at these machines and kiosks; and maintain the quality of CCTV footage.

8.5.2 Licensees should verify that adequate physical security measures are implemented at third party payment kiosks, which accept and process licensees' payment cards.

9. Systems Reliability, Availability and Recoverability

9.0.1 The reliability, availability, and recoverability of IT systems, networks and infrastructures are crucial in maintaining confidence and trust in the operational and functional capabilities of a licensee. When critical systems fail, the disruptive impact on the licensee's operations or customers will usually be severe and widespread and the institution may suffer serious consequences to its reputation.

9.0.2 As all systems are vulnerable, licensees should define their recovery and business resumption priorities. At least annually a licensee should also test its contingency procedures in order to minimize disruptions of its business arising from a serious incident.

9.1 Systems Availability

9.1.1 Important factors associated with maintaining high system availability are adequate capacity, reliable performance, fast response time, scalability, and swift recovery capability. Licensees should ensure that their business continuity plans are updated, and that the recovery site can adequately support all key systems in the production environment. Additional guidance on business continuity activities is outlined in section 4.3, Business Continuity Management, of the **Operational Risk Management Guideline.**

9.1.2 Licensees may employ a number of complex interdependent systems and network components for their IT processing. An entire system can become inoperable when a single critical hardware component or software module malfunctions or is damaged. Licensees should:

a. Develop built-in redundancies to reduce single points of failure which can bring down the entire network; and
b. Include a strategy to have standby hardware, software and network components that are necessary for their recovery.

9.1.3 Licensees should achieve high availability[18] for critical systems[19].

9.2 Data Backup Management

9.2.1 Licensees should develop a data backup strategy for the storage of critical information.

9.2.2 As part of the data backup and recovery strategy, licensees may implement specific data storage architectures such as Direct-Attached Storage (DAS), Network- Attached Storage (NAS) or Storage Area Network (SAN) sub-systems connected to production servers. In this regard, processes should be in place to review the architecture and connectivity of sub disk storage systems for single points of failure and fragility in functional design and specifications, as well as the technical support by service providers.

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

[18] Other than during periods of planned maintenance, licensee should enhance their systems and infrastructure resiliency by deploying suitable solutions. E.g. active – setup, for these systems to minimize downtime

[19] Critical system means a system where by the failure would cause significant disruption to the operations of a licensee or materiality impact to the licensee's service to its customers. "System" means any hardware, software, network or IT component.

9.2.4 Licensees should encrypt backup tapes and disks, including USB disks, containing sensitive or confidential information before they are transported offsite for storage.

9.3 Disaster Recovery Plan

9.3.1 In formulating and constructing a rapid recovery plan, licensees should include a scenario analysis to identify and address various types of contingency scenarios. Licensees should plan for the recovery from at minimum, the following disruptive events:

- Natural events such as hurricanes, floods, other severe weather conditions;
- Technical events such as power outage and fluctuations, communication failure, equipment and software failure, Licensees should consider scenarios such as major system outage, which may be caused by system faults, hardware malfunction, operating errors or security incidents, as well as a total incapacitation of the primary data center;
- Malicious activities including network security attacks, assaults and public riots; and
- Fires.

9.3.2 IT incidents, if handled inappropriately, may escalate into situations that have a severe impact on licensees' operations or its customers. Licensees should evaluate their recovery plan and incident response procedures at least annually and update them as and when changes to business operations, systems and networks occur.

9.3.3 To strengthen recovery measures relating to large-scale disruptions and to achieve risk diversification, Licensees should implement adequate backup and recovery capabilities at the individual system or application cluster level. Licensees should consider inter-dependencies between critical systems in drawing up their recovery plan and conducting contingency tests.

9.3.4 Licensees should define system recovery and business resumption priorities and establish specific recovery objectives including Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for IT systems and applications. RTO is the duration of time, from the point of disruption, within which a system should be restored. RPO refers to the acceptable amount of data loss for an IT system should a disaster occur.

9.3.5 Insofar as the size of the institution allows, licensees should establish a recovery site that is sufficiently outside the perimeter of the primary site. This should enable the restoration of critical systems and resumption of business operations, in the event a disruption occurs at the primary site.

9.3.6 The required speed of recovery will depend on the criticality of resuming business operations, the type of services and whether there are alternative ways and processing means to maintain adequate continuing service levels to satisfy customers. Licensees may wish to explore recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance their recovery capability.

9.3.7 The resiliency and robustness of critical systems which are outsourced to offshore service providers is highly dependent on the stability and availability of cross-border network links. To minimize impact on business operations in the event of a disruption, licensees should ensure cross-border network redundancy, insofar as possible.

9.4 Disaster Recovery Testing

9.4.1 During a system outage, licensees should refrain from adopting impromptu and untested recovery measures over pre-determined recovery actions that have been rehearsed and approved by management. Untested recovery measures carry high operational risks as their effectiveness has not been verified through rigorous testing and validation.

9.4.2 Licensees should test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.

9.4.3 Licensees should test the recovery dependencies between systems. Bilateral or multilateral recovery testing should be conducted where networks and systems are linked to specific service providers and vendors.

9.4.4 Licensees should involve its business users in the design and execution of comprehensive test cases to verify that recovered systems function properly. Licensees should also participate in disaster recovery tests that are conducted by its service provider(s), including those systems which are located offshore.

9.5 Data Center Protection

9.5.1 As Licensees' critical systems and data are concentrated and maintained in the Data Center (DC), it is important that the DC is resilient and physically secured from internal and external threats.

9.5.2 The purpose of a physical Threat and Vulnerability Risk Assessment (TVRA) is to identify security threats to and operational weaknesses in a DC in order to determine the level and type of protection that should be established to safeguard it. Each licensee should base its TVRA on various possible scenarios of threats which include theft, explosives, arson, unauthorized entry, external attacks and insider sabotage.

9.5.3 Licensees should include in the scope of the TVRA, a review of the DC's perimeter and surrounding environment, as well as the building and DC facility. Licensees should also review daily security procedures, critical mechanical and engineering systems, building and structural elements as well as physical, operational and logical access controls.

9.5.4 When selecting a DC provider, Licensees should obtain and assess the TVRA report on the DC facility. Licensees should verify that TVRA reports are current and that the DC provider is committed to address all material vulnerabilities identified. For Licensees that choose to build their own DC, an assessment of threats and vulnerabilities should be performed at the feasibility study stage.

9.5.5 Licensees should limit access to DC to authorized staff only. Access should only be granted to the DC on a need to have basis. Physical access of staff to the DC should be revoked immediately if it is no longer required. Licensees should deploy security systems and surveillance tools, where appropriate, to monitor and record activities that take place within the DC. Licensees should establish physical security measures to prevent unauthorized access to systems, equipment racks and tapes.

9.5.6 For non-DC personnel such as vendors, system administrators or engineers, who may require temporary access to the DC to perform maintenance or repair work, licensees should ensure that there is proper notification of and approval for such personnel for such visits. Licensees should ensure that visitors are accompanied at all times by an authorized employee while in the DC.

9.5.7 Licensees should ensure that the perimeter of the DC, DC building, facility, and equipment room are physically secured and monitored. Licensees should employ physical, human and procedural controls (e.g. security guards, card access systems, mantraps and bollards) where appropriate.

9.6 Data Center Resiliency

9.6.1 To achieve DC resiliency, licensees should assess the redundancy and fault tolerance in areas such as electrical power, air conditioning, fire suppression and data communications.

9.6.2 Licensees should rigorously control and regulate the environment within a DC. Monitoring of environmental conditions, such as temperature and humidity, within a DC is critical in ensuring uptime and system reliability. Licensees should promptly escalate any abnormality detected to management and resolve the abnormality in a timely manner.

9.6.3 Licensees should implement appropriate fire protection and suppression systems in the DC to control a full-scale fire if it occurs. Licensees should install smoke detectors and hand-held fire extinguishers in the DC and implement passive fire protection elements, such as fire walls around the DC, to restrict the spread of a fire to a portion of the facility.

9.6.4 To ensure there is sufficient backup power, licensees should install backup power consisting of uninterruptible power supplies, battery arrays, and/or diesel generators.

9.7 Cyber-Attack Exercises

9.7.1 Licensees should carry out regular scenario-based cyber exercises to validate its response and recovery, as well as communication plans in case of a cyber-attack. These exercises could include social engineering, table-top[20], cyber range[21] or adversarial attack simulation[22] exercises.

9.7.2 Based on the type and objectives of the exercise, the licensee should involve all relevant stakeholders, *inter alia* Senior Management, business functions, corporate communications, crisis management team, service providers, and technical staff responsible for cyber threat detection, response and recovery.

9.7.3 The objectives, scope and rules of engagement should be defined before the commencement of the exercise. To ensure that the activities executed don't disrupt the licensee's production systems, the exercise must be closely supervised and performed in a controlled environment.

9.7.4 Licensees should bear in mind that the simulation of realistic adversarial simulation attacks ought to be designed based on plausible cyber-attacks, and therefore should design the exercises by using threat intelligence that is

[20] Table-top exercise is a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario

[21] Cyber ranges are interactive, simulated representations of an organization's local network, IT system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and secure environment for product development and security posture testing

[22] An adversarial attack simulation exercise provides a more realistic picture of a licensee's capability to prevent, detect and respond to real adversaries by simulating the tactics, techniques and procedures of real-world attackers to target people, processes and technology underpinning the licensee's critical business functions or services

relevant to their IT environment. This technique facilitates the identification of threat actors who are highly probable to pose a threat to the licensee; as well as to assist in the identification of the tactics, techniques and procedures most likely to be used in such attacks.

10. Management of IT Outsourcing Risks[23]

10.0.1 IT outsourcing comes in many forms. Some of the most common types of IT outsourcing are in systems development and maintenance, support to DC operations, network administration, disaster recovery services, application hosting, and cloud computing. Outsourcing can involve the provision of IT capabilities and facilities by a single third party or multiple vendors located in Barbados or abroad.

10.0.2 The Board and Senior Management should fully understand the risks associated with IT outsourcing.

10.0.3 Licensees should require the service provider to implement security policies, procedures, and controls that are at least as stringent as they would expect for their own operations. To this end licensees should ensure:

a. The effectiveness of the risk-mitigating measures as defined by their risk management framework;
b. The continuity of technology services and information systems;
c. That contracts and service level agreements (both for normal circumstances as well as in the event of service disruption), include minimum cyber resilience requirements as well as security incident handling procedures for escalation and reporting;
d. Third parties submit reports that provide assurance of the level of compliance with the cyber resilience objectives, measures and performance targets as defined by the licensee. These reports should be submitted at least annually or when major changes have been implemented by the service provider; and
e. The appropriate due diligence is conducted by service providers on the third parties as applicable.

10.0.4 All parties concerned, including those from the service provider, should receive regular training in activating the contingency plan and executing recovery procedures.

10.0.5 Licensees should have contingency plans in place based on credible worst-case scenarios for service disruptions to prepare for the possibility that their current

[23] This section should be read in conjunction with the Bank issued Outsourcing Guideline.

service provider may not be able to continue operations or render the services required. The plan should incorporate identification of viable alternatives for resuming the IT operations elsewhere.

10.1 Sub-Outsourcing of Critical or Important Functions

10.1.1 Sub-outsourcing, also known as chain-outsourcing, refers to a situation where the service provider under an outsourcing arrangement further transfers an outsourced function or part of an outsourced function to another service provider or sub-contractor.

10.1.2 It is important for licensees to note that they remain fully responsible for the outsourced function and that compliance with regulatory requirements in the case of out sub-outsourcing is necessary as it is with outsourcing.

10.1.3 Licensees are advised that they should only agree to sub-outsourcing of critical or important functions, if the sub-contractor undertakes to:

a) Comply with all applicable laws, regulatory requirements and contractual obligations; and
b) Grant the licensee and Bank the same contractual rights of access and audit as those granted by the service provider.

10.1.4 Licensee should ensure that the service provider specify ex ante notification in the event that critical or important functions plan to be outsourced. Licensees should always have the right to terminate the contract if planned changes to services, including such changes caused by sub-outsourcing, would have an adverse effect on the risk assessment of the outsourced services.

10.1.5 The outsourcing agreement for critical or important functions should set out whether the sub-sourcing of a critical or important function, or material parts thereof, is permitted. If so, the conditions as specified in section 10.2.6 should be adhered to.

10.1.6 If sub-outsourcing of critical or important functions is permitted, the written agreement should:

a) Specify any types of activities that are excluded from sub-outsourcing;

b) Specify the conditions to be compiled with in the case of sub-outsourcing;

c) Specify that the service provider is obliged to oversee those services

that it has sub-contracted to ensure that all contractual obligations between the service provider and the licensee are continuously met;

d) Require the service provider to obtain prior specific or general written authorization from the licensee before sub-outsourcing data;

e) Include an obligation of the service provider to inform the licensee of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This would allow the licensee to carry out a risk assessment of the proposed changes and to object to changes before they come into effect;

f) Ensure that the licensee maintains the right to object to intended sub-outsourcing, or material changes or that explicit approval is required;

g) Ensure that the licensee has the contractual right to terminate the agreement with the service provider in the event sub-outsourcing materially increases the risks for the licensee or where the service provider sub-outsources without notifying the licensee.

10.1.7 Licensees should ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined and agreed by both counterparts.

10.2 Cloud Computing

10.2.1 Cloud services ("CS") operated by service providers are considered a form of outsourcing that institutions apply to enhance their operations, while reaping the benefits of CS' scalable, standardized and secured infrastructure.

10.2.2 The types of risks in CS that confront institutions are not distinct from that of other forms of outsourcing arrangements. Institutions should perform the necessary due diligence and apply sound governance and risk management practices articulated in this guideline when subscribing to CS.

10.2.3 Licensees should be aware of CS' typical characteristics such as multi-tenancy, data commingling and the higher propensity for processing to be carried out in multiple locations. Hence, licensees should take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. In particular, institutions should ensure that the service provider possesses the ability to clearly identify and segregate customer data using strong physical or logical controls. The service provider should have robust access controls in place to protect

customer information

10.2.4 Licensees are ultimately responsible and accountable for maintaining oversight of CS and managing the attendant risks of adopting CS, as in any other form of outsourcing arrangements. A risk-based approach should be taken by institutions to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the CS.

11. Internet of Things

11.0.1 Internet of Things (IoT) includes any electronic devices, such as smart phones, multi-function printers, security cameras and smart televisions, which can be connected to the licensee's network or the Internet. Privacy of IoT device end-users can no longer be seen as an add-on to existing products or services. As with all information assets, the licensee should maintain an inventory of all its IoT devices, including information such as the networks which they are connected to and their physical locations.

11.0.2 Many IoT devices are designed without or with minimal security controls. If compromised, these devices can be commandeered and used to gain unauthorised access to the licensee's network and systems or as a launch pad for cyber-attacks on the licensee. Compromised IoT devices may additionally exfiltrate data and cause disruption of the network during such orchestrated attacks. The licensee should assess and implement processes and controls to mitigate risks arising from IoT. The network that hosts IoT devices should be secured. For instance, network access controls can be implemented to restrict network traffic to and from an IoT device to prevent a cyber threat actor from accessing the licensee's network and launching malware or DoS attacks. To further reduce IoT risks, the licensee should host IoT devices on a separate network segment from the network that provides access to the licensee's systems and confidential data.

11.0.3 The licensee should implement controls to prevent unauthorised access to IoT devices. In light of privacy risks that the use of IoT technology brings licensees should take additional measure to safeguard Personally Identifiable Information (PII).

11.0.4 Similar to other systems, the licensee should monitor IoT devices for suspicious or anomalous system activities so that prompt actions can be taken to isolate compromised devices. Security monitoring should include but is not limited to:

- Endpoint identity monitoring;
- Endpoint identity impersonation;
- Trust anchor attacks;
- Software and firmware tampering;

- Secure remote management;
- Detecting compromised endpoints;
- Service impersonation.

11.0.5 Concluding, with all new and emerging technology, a proper risk assessment, due diligence and due care needs to be taken into consideration. Technologies that may be used to further monitor technology and cyber risk developments are the application and use of artificial intelligence, machine learning and quantum computing.

12. Information and Intelligence Sharing

12.0.1 Information and intelligence sharing is one of the high-level building blocks in facilitating cyber resilience across the sector by raising awareness of cyber risk, minimising its spread and supporting a licensee's defensive capabilities and threat detection techniques.

12.0.2 Licensees may adopt a systematic unified approach to sharing information and intelligence with trusted stakeholders, which would better enable them to identify, assess, monitor and respond to cyber threats.

12.0.3 In order to achieve efficient and effective use of information and intelligence sharing opportunities, licensees may consider the below best practice approach:

i. Establish information and intelligence sharing goals and objectives that support business processes and security policies.
ii. Identify existing internal sources of cyber threat information.
iii. Specify the scope of information sharing activities.
iv. Establish information sharing rules.
v. Join and participate in information and intelligence sharing efforts
vi. Actively seek to enrich indicators by providing additional context, corrections, or suggested improvements.
vii. Use secure, automated workflows to publish, consume, analyze and act upon cyber threat information.
viii. Proactively establish cyber threat sharing agreements.
ix. Protect the security and privacy of sensitive information.
x. Provide ongoing support for information and intelligence sharing activities.