PRUDENTIAL STANDARD ON TECHNOLGY RISK MANAGEMENT FOR INSTITUTIONS LICENSED UNDER THE BANKING ACT, 2015

NOVEMBER 2022

EASTERN CARIBBEAN CENTRAL BANK

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 2382:2015
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
Availability	Property of being accessible and usable on demand by an authorised entity. Source: ISO/IEC 27000:2018

[1] 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
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
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 not 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
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

Term	Definition
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
Identify (function)	Develop the organisational understanding to manage *cyber risk* to *assets* and capabilities. Source: Adapted from NIST Framework
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	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
Incident Response Team (IRT) [also known as CERT or CSIRT]	Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle. Source: ISO/IEC 27035-1:2016
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")
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

Term	Definition
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
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
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

Term	Definition
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
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
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
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

Term	Definition
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
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 colour 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 27000:201
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 NICCS

Table of Contents

PRUDENTIAL STANDARD ON TECHNOLGY RISK MANAGEMENT FOR INSTITUTIONS LICENSED UNDER THE BANKING ACT, 2015

This Prudential Standard (The Standard) is issued by the Eastern Caribbean Central Bank (ECCB/Central Bank), in exercise of the powers conferred on it by Section 184 of the Banking Act, 2015 (hereinafter referred to as the Act)[1].

Commencement

This Standard shall come into effect on the 3rd day of January 2023.

1 Introduction

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 licensed financial institutions' (LFI) business operations have also grown in scope and complexity over the years. In most cases IT is no longer a support function for LFIs, but a key enabler for business strategies including reaching out to and meeting customer needs. LFIs offering a diversity of products and services could have their financial systems operating in multiple locations and supported by different service providers.

LFIs are also faced with the challenge of keeping pace with the needs and preferences of consumers who are becoming 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] See Section 183 of the Banking Act of Anguilla, 2015 (No 6 of 2015), as amended.

LFIs 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, LFIs should fully understand the technology 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.

2 Objective

The Technology Risk Management prudential standards aims to:

a. Set out risk management principles and best practice standards for:
   i. Establishing a sound and robust technology risk management framework;
   ii. Protecting customer data, transactions and systems; and
   iii. Strengthening system security, reliability and resilience

b. Create a standardized approach for treatment of technology and should be applied by all licensed financial institutions, and their subsidiaries, unless IT is not a significant function, or alternative measures have been taken to comply with the objectives of these standards that can be considered equally effective.

c. Provide guidance on measures that LFIs can take to mitigate the impact of security events through:
   i. The maintaining of information security capabilities that are commensurate with their technology risk levels, size and complexity;
   ii. The utilising of lessons learnt by other LFI's to bolster existing systems, practices and procedures.

The structure of this document is presented in figure 1.

Figure 1. Structure of Policy Paper Scope and Applicability

3 Scope of Application

a) These standards must be read in conjunction with the suite of Prudential Standards issued by the ECCB.

b) These standards are intended to create a standardized approach for treatment of technology and should be applied by all regulated licensed financial institutions, Financial Groups and Conglomerates in their relevant Supervisory Authority, unless IT is not a significant function, or alternative measures have been taken to comply with the objectives of these standards that can be considered equally effective.

c) Any deviation from these standards must be explained in a separate document, to be made promptly available to the ECCB upon its request.

4 Information Technology Governance

Consistent with the ECCB's Prudential Standard on Corporate Governance, the Board of Directors (the Board) of an LFI is ultimately responsible for effective oversight of all IT and cybersecurity risks, systems and processes. Both the Board and Senior Management should ensure that the LFIs IT function is capable of supporting the institution's business strategies, objectives and services in a reliable, and resilient manner.

5 Oversight of Technology Risks by the Board and Senior Management

IT is a core function for LFIs to deliver their services. When critical systems fail and users cannot access financial services their accounts, a LFI's business operations, the impact on

customers would be far reaching, with significant consequences to the LFI, including financial and reputational damage.

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

5.1 *Roles and Responsibilities*

Board of Directors

The Board's roles and responsibilities shall include, but are not limited to the following:

a. Ensuring the development of a robust cyber-risk management framework inclusive of effective internal controls and risk management practices aimed at achieving continuous security, reliability, resilience and recoverability;
b. Ensuring that the Board and Senior Management comprise person(s) with IT skills and qualifications that are commensurate with the LFI's cyber risk profile and allow for effective oversight of the IT function and management of cyber-risks;
c. Approving technology policies, standards and procedures that govern the management of technology risks and safeguard the LFI's information system assets and ensuring the regular review of the aforementioned;
d. Ensuring the development of processes to verify that standards, policies and procedures are enforced and adhered to;
e. Ensuring that staff and service providers authorised to access the IT system are formally required to keep all information confidential and sign the relevant non-disclosure agreement(s);
f. Ensuring the establishment of cyber-risk tolerance levels that are within the LFI's cyber risk profile and have minimal impact on the LFIs IT systems and overall operations.

g. Ensuring the establishment of a comprehensive enterprise wide IT security awareness training program, geared at enhancing the overall IT and IT security awareness levels in the organization and at the Board level.

Senior Management

Senior Management's roles and responsibilities shall include but are not limited to the following:

a. Implementation of the board approved cyber security strategies, policies and framework;
b. The allocation of resources required for cybersecurity management and ensure timely and regular reporting to the Board on the institution's cybersecurity posture and cyber risk status;
c. Implementing mitigation and recovery procedures and processes for cyber risk incidents, with an approach to improve the effectiveness of the institution's cyber and information security measures;
d. The discussion, assessment and reporting on cybersecurity and IT risk.
e. Developing and implementing a cybersecurity incident response plan that details the steps to be taken in the event of a security breach. The plan should include:
    i. The roles and responsibilities of staff;
    ii. Risk tolerance levels
    iii. Cybersecurity risk triggers;
    iv. Incident detection, escalation, assessment and reporting processes; and
    v. Strategies for deployment based on the threat.
f. Notifying the general public about the cybersecurity incident(s) subsequent to notifying the ECCB;
g. Notifying directly, the customer(s) whose accounts were potentially or actually compromised within seventy-two (72) hours of the discovery of the incident.
h. Implementation of a training program that ensures training is conducted and updated at least annually. All employees, including Senior Management,

should receive training on IT security policies and procedures, as well as individual responsibility for IT security and measures to protect information system assets. The training program should be reviewed and updated to ensure that the contents remain current and relevant, taking into account the evolving nature of technology as well as emerging risks. The Board of Directors should focus on awareness of the current and emerging risks associated with the use of technology, to enhance their understanding of technology risk management practices.

i. Senior management should ensure the LFI's IT strategy is in alignment with the institution's overall business strategy, as well as, monitor and evaluate existing and future trends in technology that may impact the business strategy, including monitoring of overall industry trends.

5.2 *IT Policies, Standards and Procedures*

5.2.1 LFIs should establish IT policies, standards, and procedures to manage technology risks and safeguard information system assets[2] in the organization in line with current industry standards, approved by Senior Management or the LFI's Board (or an appropriate committee thereof), setting forth the LFI's protection of its information systems and information processed by those information systems.

5.2.2 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.

5.2.3 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.

5.2.4 All LFIs that rely heavily on their IT systems for their daily operations should establish a cybersecurity policy based on the LFI's risk

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

assessment and mitigate the identified cyber risk threats commensurate with its risk appetite.

5.3 *People Selection Process*

5.3.1 Careful selection of staff, vendors and contractors is crucial to minimize technology risks due to system failure, internal sabotage or fraud. As people play an important role in managing systems and processes in an IT environment, LFIs should implement a screening process that is comprehensive and effective. At a minimum the process should include skills testing, checks and verification of resumes, request for proposals, due diligence and interviews.

5.3.2 Staff, vendors and contractors, who are authorized to access an LFI's systems, should be required to adhere to the LFI's information system security policy.

5.4 *IT Security Awareness*

5.4.1 A comprehensive IT security awareness training program should be established to enhance the overall IT security awareness levels within the LFI's organizational structure. The training program should include information on IT security policies and standards as well as each employee's individual responsibility to protect information system assets. Each employee should be made aware of the applicable laws, regulations, and guidelines pertaining to the usage, deployment and access to IT resources.

5.4.2 The IT security awareness training program should be conducted and updated at least annually.

5.4.3 At least annually the IT security awareness training program should be reviewed and updated where necessary, to 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

6 Technology Risk Management Framework

A technology risk management framework should be established to manage technology 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.

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

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

6.1 *Information System Assets*

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

6.1.2 LFIs 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 classification processes should be in place to prescribe a criticality assessment, ownership, and handling.

6.2 *Risk Identification*

6.2.1 Risk identification entails the determination of the threats and vulnerabilities to an LFI'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.

6.2.2 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 LFI and its information systems.

6.2.3 Cyber security 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 LFI with consequential losses for all parties affected. LFIs should be vigilant in identifying and monitoring such risks as it is a crucial step in the risk containment exercise.

6.3 *Risk Assessment*

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

6.3.2 LFIs should analyze the impact and likelihood of the threats and vulnerabilities that could cause harm to the organization, including most likely scenarios.

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

6.3.4 LFIs should maintain/include a cybersecurity program designed to protect the confidentiality, integrity and availability of the LFI's information systems. The cybersecurity program should be based on the LFI's assessment of technology risk and should be designed to perform the following core cybersecurity functions:

a) Identify and assess internal and external technology risks that may threaten the security and integrity of information stored on the LFI's information systems;
b) Use defensive infrastructure and the implementation of policies and procedures to protect the LFI's information systems, and the 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.

6.4 *Risk Treatment*

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

6.4.2 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. In addition, taking insurance cover for various insurable risks, including recovery and restitution costs should be considered.

6.4.3 As it may not be practical to address all known risks simultaneously or in the same timeframe, LFIs should give priority to threat and vulnerability pairings that could cause significant harm or impact to a LFI's operations. The costs of risk controls should be balanced against the benefits to be derived.

6.4.4 It is imperative that LFIs 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, LFIs should balance the impact to all stakeholders against the benefits to be derived.

6.4.5 LFIs 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.

6.5 **Risk Monitoring and Reporting**

6.5.1 LFIs 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. LFIs should update the

risk register periodically, and institute a monitoring and review process for continuous assessment and treatment of risks.

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

6.5.3 Risk parameters may shift as the IT environment and delivery channels change. Thus, LFIs should review and update the risk processes accordingly, and conduct a periodic evaluation of risk-control methods that includes an assessment of the adequacy and effectiveness of IT controls and risk management processes.

6.5.4 Management of the IT function should review and update its IT risk control and mitigation approach, taking into account changing circumstances and variations in the LFIs risk profile.

7 Operational IT Risk Guidelines

Many systems fail due to poor system design and implementation, as well as inadequate testing. LFIs should identify system deficiencies and defects at the system design, development and testing phases. Moreover, LFIs 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. Ongoing attention should be given to the sufficiency of the IT security measures in place and risk management throughout the project life cycle.

7.1 *IT Project Management*

7.1.1 In establishing a project management framework, LFIs should ensure that tasks and processes for developing or acquiring new systems include project risk assessment and classification, critical success factors for each project phase, definition of project milestones and deliverables. LFIs should clearly define in the project management

framework, the roles and responsibilities of staff involved in the project;

7.1.2 LFIs should 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.

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

7.1.4 LFIs 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.

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

7.2 *System Acquisition*

7.2.1 LFIs should establish standards and procedures for vendor evaluation and selection to ensure the selected vendor is qualified and able to meet its project requirements and deliverables. The level of assessment and due diligence performed should be commensurate with the criticality of the project deliverables to the LFI.

7.2.2 LFIs should ensure that the hardware and software specifications used during project implementation, meets or exceeds the minimum specifications agreed to with the vendors.

7.2.3 It is important that the LFI assesses the robustness of the vendor's software development and quality assurance practices, and ensures stringent security practices are in place to safeguard and protect any sensitive data the vendor has access to over the course of the project. Any vendor access to the LFI's IT systems should be controlled and monitored.

7.2.4 If a project involves a commercial off-the-shelf solution that does not meet the LFI's security requirements, the LFI should assess the risks and ensure adequate mitigating controls are implemented to address the risks before the solution is deployed.

7.2.5 The LFI should assess if a source code escrow agreement should be in place, based on the criticality of the acquired software to the LFI's business, so that the LFI can have access to the source code in the event that the vendor is unable to support the LFI. Suitable alternatives to replace the software should be identified if an escrow agreement could not be implemented.

7.3 *System Security Requirements and Testing*

7.3.1 LFIs 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.

7.3.2 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.

7.3.3 LFIs 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

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

operations are affected by the system changes should review and sign off on the outcome of the tests.

7.3.4 LFIs should conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces. In the case that an LFI deviates from this decision, LFIs should document exceptions properly and have them available to the ECCB upon request. In case no prior penetration testing is possible, penetration testing should be performed within a reasonable timeframe, explained and documented. LFIs should also perform continuous vulnerability scanning of external and internal network components that support the changed and current system landscape.

7.4 *End User Development*

7.4.1 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 LFI and customers. LFIs should perform an assessment to ascertain the importance of these applications to the business.

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

7.4.3 LFIs should review and test based on their risk assessment end user developed program codes, scripts and macro's before they are used so as to ensure the integrity and reliability of the applications.

7.5 *IT Audit*

7.5.1 Audit plays an important role to assess the effectiveness of the controls, risk management and governance process at the LFI. As technology risks evolve with the growing complexity of the IT environment, there is an increasing need for LFIs to develop effective internal control systems to manage technology risks.

7.5.2 IT audit provides the Board and Senior Management with an independent and objective opinion of the adequacy and effectiveness

of the LFI's risk management, governance and internal controls relative to its existing and emerging technology risk.

7.5.3 A comprehensive set of auditable areas for technology risk should be identified so that an effective risk assessment could be performed during audit planning. Auditable areas should include all IT operations, functions and processes.

7.5.4 The frequency of IT audits should be commensurate with the criticality of and risk posed by the IT information asset, function or process.

7.5.5 The LFI should ensure its IT auditors have the requisite level of competency and skills to effectively assess and evaluate the adequacy of IT policies, procedures, processes and controls implemented.

7.5.6 LFIs 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.

7.6 *Audit Planning and Remediation Tracking*

7.6.1 LFIs should ensure that the scope of IT assessment in its audit plan is comprehensive and includes all critical IT operations. The audit plan should be approved by the Audit Committee of the Board.

7.6.2 LFIs 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.

8 IT Service Management

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. 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.

8.1 *Change Management*

8.1.1 LFIs should establish a change management process to ensure that changes to production systems are assessed, approved, implemented, and reviewed in a controlled manner.

8.1.2 The change management process should apply to changes pertaining to system and security configurations, patches for hardware devices and software updates

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

8.1.4 LFIs 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. LFIs should develop and document appropriate test plans for the impending change. LFIs should also obtain test results with user sign-offs prior to the migration.

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

8.1.6 To minimize risks associated with changes, LFIs should perform backups of affected systems or applications prior to the change. LFIs s 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. LFIs should establish alternative recovery options to address situations where a change does not allow a LFI to revert to a prior status.

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

8.2 *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.

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

8.2.2 LFIs should closely monitor vendor and developers' access to all their environments.

8.2.3 Where controls in the non-production environment are different or less stringent from those in the production environment, LFIs 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.

8.2.4 Segregation of duties should be enforced as far possible 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, LFIs should document and explain this process as well as present a suitable alternative.

8.2.5 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.

8.3 *User Access Management*

8.3.1 LFIs 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. LFIs should ensure that the resource owner duly authorizes and approves all requests to access IT resources.

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

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

8.3.4 LFIs 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.

8.3.5 Passwords represent the first line of defense, and if not implemented appropriately, they can be the weakest link in the organization. Thus, LFIs 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.

8.3.6 LFIs should ensure that no one has concurrent access to both production systems and backup systems, particularly data files and computer facilities. LFIs 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.

8.4 *Privileged Access Management*

8.4.1 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. LFIs should apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions, taking into account insider threat.

8.4.2 LFIs 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.

8.5 *Remote Access Management*

8.5.1 Remote access allows users to connect to the LFI's internal network via an external network to access the LFI'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 LFI's IT environment.

8.5.2 The LFIs should only allow remote access to the LFI's information assets from devices that have been secured, hardened and fully patched according to the LFI's endpoint security standards.

8.5.3 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 properly.

8.5.4 IT Security awareness remains critical for users that are new to the technology usage to minimize exposure to phishing and social engineering.

8.5.5 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.

8.6 *Incident Response and Management*

8.6.1 An IT incident occurs when there is an unexpected disruption to the standard delivery of IT services. LFIs should appropriately manage such incidents to avoid a situation of mishandling that result in a prolonged disruption of IT services or further aggravation.

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

8.6.3 It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, LFIs may delegate the function of determining and assigning incident severity levels to a centralized technical helpdesk function. LFIs 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.

8.6.4 LFIs 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 security incidents[5], should be tested on a regular basis.

8.6.5 LFIs should form a computer emergency response team, comprising staff with the necessary technical and operational skills to handle major incidents.

8.6.6 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 so that the decision to activate the disaster recovery plan can be made on a timely basis. LFIs should inform the ECCB promptly if a major incident occurs with due regard of the requirements as stipulated in these standards on incident response and management.

8.6.7 In the event of a disruption or emergency, and during the implementation of the BCPs, LFIs should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the competent authorities when required by national regulations, and also relevant providers (outsourcing providers or third party providers) are informed in a timely and appropriate manner.

8.6.8 The maintenance of customer confidence throughout a crisis or an emergency situation is of great importance to the reputation and soundness of a LFI. LFIs should include in their incident response

5 Examples of security incidents include virus outbreak, malware infiltration, systems hacking, account impersonation or compromise, phishing attack, internal sabotage or denial of service attacks.

procedures a predetermined action plan to address public relations issues.

8.6.9 LFIs 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.

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

8.6.11 LFIs should include in their incident report an executive summary of the incident, an analysis of root causes which triggered the event, its impact as well as measures taken to address the root cause and consequences of the event.

8.6.12 LFIs should adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution. Each LFI should notify the ECCB as promptly as possible in the event that a security breach or major incident has occurred.

8.6.13 Cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the LFI should also be reported. Annually each LFI should revise their Cybersecurity program where it has identified areas, systems or processes that require material improvement, updating or redesign. LFIs 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 ECCB.

8.6.14 In order to effectively manage incidents, LFIs should have a methodology for prioritizing such as using the Impact vs Urgency matrix. Impact can be defined as the effect the incident has on a business while Urgency can be defined as the length of time that the business is willing to wait for problem resolution.

LFIs should employ the use of an established industry framework for managing incidents.

8.6.15 In theory, 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. LFIs have to agree on what constitutes a major incident for themselves.

8.7 *Problem Management*

8.7.1 The LFI should establish problem management process and procedures to determine and resolve the root cause of incidents to prevent the recurrence of similar incidents.

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

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

9 Operational Infrastructure Security Management

The IT landscape is vulnerable to various forms of cyber-attacks[6] and the frequency and malignancy of attacks are increasing. It is imperative that LFIs implement security solutions at the data, application, database, operating systems and network layers to adequately address and contain these threats.

Appropriate technological measures should be implemented to protect sensitive or confidential information such as customer personal, account and transaction data which

6 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.

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

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 [7] (APIs) and Keys from introduction till retirement.

9.1 *Data Loss Prevention*

9.1.1 Internal sabotage, clandestine espionage or furtive attacks by trusted staff, contractors and vendors are potentially among the most serious risks that LFIs 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 a LFI's systems, operations and internal controls have a significant advantage over external attackers. A successful attack not only jeopardizes customer confidence in a LFI's internal control systems and processes but also causes real financial loss when proprietary information is divulged. LFIs should identify important data and adopt adequate measures to

[7] APIs are access points that allow user and program interaction with an application.

detect and prevent unauthorized access, copying or transmission of confidential information.

9.1.2 LFIs 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.

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

9.1.4 LFIs should not use unsafe internet services such as social media sites or internet storage sites to communicate or store confidential information. LFIs should implement measures to manage and detect the use of such services within its organization.

9.1.5 For the purpose of exchanging confidential information with external parties, LFIs should take utmost care to preserve the confidentiality and integrity of information. For this purpose, LFIs 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. LFIs should send the encryption key via a separate transmission channel to the intended recipients. Alternatively, LFIs may choose other secure

means to exchange confidential information with its intended recipients.

9.1.6 Confidential information stored on IT systems, servers, and databases should be encrypted, where possible, and protected through strong access controls, bearing in mind the principle of "least privilege"[8].

9.1.7 LFIs 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, LFIs should take into consideration security requirements of the data residing on the media.

9.2 *Technology Refresh Management*

9.2.1 To facilitate the tracking of IT resources, LFIs 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.

9.2.2 LFIs 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. LFIs 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.

9.2.3 LFIs should establish a technology refresh plan to ensure that systems and software are replaced in a timely manner. LFIs should conduct a risk assessment for systems approaching EOS dates to assess the risks

8 Least privilege is defined as assigned privileges on a "need-to-have" basis.

of continued usage and establish effective risk mitigation controls where necessary.

9.3 *Networks and Security Configuration Management*

9.3.1 LFIs 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. LFIs 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.

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

9.3.3 LFIs should deploy anti-malware software to servers, if applicable, and workstations. LFIs 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.

9.3.4 LFIs 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. LFIs should deploy firewalls, or other similar measures, within internal networks to minimize the impact of security exposures originating from third party or remote systems, as well as from the internal trusted network. On an annual basis, LFIs should also back up and review rules on network security devices to determine that such rules are still appropriate and relevant.

9.3.5 LFIs 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.

9.3.6 A review of the LFI'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 cyber security vulnerabilities.

9.4 *Vulnerability Assessment and Penetration Testing*

9.4.1 Vulnerability Assessment (VA) is the process of identifying, assessing and discovering security vulnerabilities in a system. LFIs 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.

9.4.2 LFIs 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.

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

9.4.4 LFIs should carry out penetration tests in order to conduct an in-depth evaluation of the cyber security posture of the system through simulations of actual attacks on the system. LFIs should 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.

9.5 *Patch Management*

9.5.1 LFIs 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, LFIs should establish the implementation timeframe for each category of security patches.

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

9.6 *Security Monitoring and Detection*

9.6.1 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, LFIs should establish appropriate security monitoring systems and processes.

9.6.2 LFIs 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 LFI against network intrusion attacks as well as to provide alerts when an intrusion occurs.

9.6.3 LFIs 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. LFIs should include capacity management to

support business functions, and ensure that indicators such as performance, capacity, and utilization are monitored and reviewed.

9.6.4 LFIs 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.

9.6.5 LFIs should review security logs of systems, applications, and network devices for anomalies at least monthly. LFIs 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.

9.6.6 To enhance the effectiveness of security monitoring, the LFI 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.

9.6.7 LFIs should adequately protect and retain system logs to facilitate any future investigation. When determining the log retention period, LFIs should take into account statutory requirements for document retention and protection.

10 Online Financial Services[9]

Whilst the internet presents opportunities for LFIs to reach new markets and expand its range of products and services, being an open network, it also brings about security risks that are more sophisticated and dynamic than closed networks and proprietary delivery channels. LFIs should be cognizant of risks that are brought about as a result of offering financial services via the internet platform.

9 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.

LFIs should clearly identify risks associated with the types of services being offered in the risk management process. LFIs 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.

10.1 *Online Systems Security*

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

10.1.2 LFIs 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.

10.1.3 The ECCB expects LFIs 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).

10.1.4 LFIs should ensure that information processed, stored or transmitted between their LFI and their 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. LFIs' should implement physical and logical access security to allow only authorized personnel to access its systems. LFIs should also implement appropriate processing and transmission controls to protect the integrity of systems and data.

10.1.5 LFIs should implement monitoring or surveillance systems so that it is alerted to any abnormal system activities[10], transmission errors or unusual online transactions. LFIs should establish a follow-up

10 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.

process to verify that these issues or errors are adequately addressed subsequently.

10.1.6 LFIs should maintain high resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment). LFIs 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).

10.1.7 LFIs should implement multi-factor authentication11 (MFA) at login for all types of online financial systems and transaction-signing for authorizing transactions. The primary objectives of two-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 LFIs and their customers.

10.1.8 LFIs should also take appropriate measures to minimize exposure to other forms of cyber-attacks such as middleman attack which is more commonly known as a man-in-the-middle attack12 (MITMA), man-in-the browser attack or man-in-the application attack.

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

11 Two-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).

12 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.

customers on security measures that are put in place to protect their customers in an online environment.

10.1.10 The LFI should advise their customers on the means to detect unauthorised transactions and to report promptly security issues, suspicious activities or suspected fraud to the LFI.

11 Mobile Online Services and Payments Security

a) 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).

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

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

d) LFIs should educate their customers on security measures to protect their own mobile devices from malware and other errant software which cause malicious damage and have harmful consequences.

11.1 *Bank specific: Payment Card Security (ATM's, Credit and Debit Cards)*

11.1.1 Payment cards [13] allow cardholders the flexibility to make purchases wherever they are. 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.

11.1.2 Payment cards exist in many forms; with magnetic stripe cards posing the highest security risks. LFIs, as they are in the position to issue cards should follow international standards of migrating away from magnetic stripe card types to other, safer, methods (e.g. EMV chip supported card transactions).

11.1.3 Types of payment card fraud include counterfeit, lost/stolen, card-not received [14] ("CNR") and card-not-present [15] ("CNP") fraud. LFIs should monitor payments patterns for insider threat.

11.2 *Banks specific: Payment Card Fraud*

11.2.1 LFIs that provide payment card services should implement adequate safeguards to protect sensitive payment card data. LFIs should ensure that sensitive payment card data is (PCI compliant) encrypted to ensure the confidentiality and integrity of these data in storage and

13 For the purpose of this document, "payment cards" refer to ATM, credit, charge and debit cards.
14 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.
15 Card-not-present fraud involves the use of stolen or compromised card details to make purchases over the internet, phone or mail order.

transmission, and the processing of sensitive or confidential information is done in a secure environment.

11.2.2 LFIs should deploy secure methods to store sensitive payment card data. LFIs 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, LFIs should ensure that adequate controls are implemented to manage these transactions.

11.2.3 LFIs 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. LFIs should perform regular security reviews of the infrastructure and processes being used by their service providers and merchants.

11.2.4 LFIs should ensure that security controls are implemented at payment card systems and networks.

11.2.5 To enhance card payment security, LFIs should promptly notify cardholders via transaction alerts when withdrawals / charges exceeding customer-defined thresholds are made on the customers' payment cards. LFIs should implement robust fraud detection systems with behavioral scoring or equivalent; and correlation capabilities to identify and curb fraudulent activities. LFIs 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.

11.2.6 LFIs should follow up on transactions exhibiting behavior which deviates significantly from a cardholder's usual card usage patterns.

LFIs should investigate these transactions and obtain the cardholder's authorization prior to completing the transaction.

11.3 *Bank: ATMs and Payment Kiosks Security*

11.3.1 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.

11.3.2 To secure consumer confidence in using these systems, LFIs should put in place the following measures to counteract fraudsters' attacks on ATMs and payment kiosks:

(a) 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 the LFI 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.

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

12 Systems Reliability, Availability and Recoverability

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 LFI. When critical systems fail, the disruptive impact on the LFI's

operations or customers will usually be severe and widespread and the LFI may suffer serious consequences to its reputation.

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

12.1 *Systems Availability*

12.1.1 Important factors associated with maintaining high system availability are adequate capacity, reliable performance, fast response time, scalability, and swift recovery capability. LFIs should ensure that the business continuity plans are updated, and that the recovery site can support the new production environment.

12.1.2 LFIs 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. LFIs should develop built-in redundancies to reduce single points of failure which can bring down the entire network. LFIs should include a strategy to have standby hardware, software and network components that are necessary for their recovery.

12.1.3 LFIs should achieve high availability16 for critical systems17.

16 Other than during periods of planned maintenance, FIs should enhance their systems and infrastructure resiliency by deploying suitable solutions, e.g., active-active setup, for these systems to minimize downtime.

17 Critical system means a system, the failure which will cause significant disruption to the operations of a FI or materially impact the FI's service to its customers. "System" means any hardware, software, network or IT component which is part of an IT infrastructure

12.2 *Data Backup Management*

12.2.1 LFIs should develop a data backup strategy for the storage of critical information.

12.2.2 As part of the data backup and recovery strategy, LFIs 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.

12.2.3 LFIs 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.

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

12.3 *Disaster Recovery Plan*

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

(a) Natural events such as hurricanes, floods, other severe weather conditions;

(b) Technical events such as power outage and fluctuations, communication failure, equipment and software failure; LFIs 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.

(c) Malicious activities including network security attacks, frauds, assaults and public riots;

(d) Pandemics; and

(e) Fires.

12.3.2 IT incidents, if handled inappropriately, may escalate into situations that have a severe impact on LFIs' operations or its customers. LFIs 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.

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

12.3.4 LFIs 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.

12.3.5 Insofar the size of the institution allows so, LFIs should establish a recovery site that is sufficiently outside perimeter of primary site to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site.

12.3.6 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. LFIs may wish to explore

recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance their recovery capability.

12.3.7 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, LFIs should ensure cross-border network redundancy, insofar as possible.

12.4 *Disaster Recovery Testing*

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

12.4.2 LFIs 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.

12.4.3 LFIs 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.

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

12.5 *Data Center Protection*

12.5.1 As LFIs' 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.

12.5.2 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. An LFI should base its TVRA on various possible scenarios of threats which include theft, explosives, arson, unauthorized entry, external attacks and insider sabotage.

12.5.3 LFIs 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. LFIs should also review daily security procedures, critical mechanical and engineering systems, building and structural elements as well as physical, operational and logical access controls.

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

12.5.5 LFIs should limit access to DC to authorized staff only. LFIs should only grant access 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. LFIs should deploy security systems and surveillance tools, where appropriate, to monitor and record activities that take place within the DC. LFIs should establish physical security measures to prevent unauthorized access to systems, equipment racks and tapes.

12.5.6 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, LFIs should ensure that there is proper notification of and approval for such personnel for such visits. LFIs should ensure that visitors are accompanied at all times by an authorized employee while in the DC.

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

12.6 *Data Center Resiliency*

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

12.6.2 LFIs 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. LFIs should promptly escalate any abnormality detected to management and resolve the abnormality in a timely manner.

12.6.3 LFIs should implement appropriate fire protection and suppression systems in the DC to control a full-scale fire if it occurs. LFIs 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.

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

12.7 *Cyber Threat Intelligence and Information Sharing*

12.7.1 To maintain good cyber situational awareness, the LFIs should establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the LFI's business and IT environment. Cyber-related information would include cyber events, cyber threat intelligence and information on system vulnerabilities.

12.7.2 LFIs should procure cyber intelligence monitoring services. As cyber threat information sharing is an important component of cyber resilience within the financial ecosystem, LFIs should actively participate in cyber threat information-sharing arrangements with

trusted parties to share and receive timely and actionable cyber threat information.

12.7.3 LFIs are required to establish an Information Security User Group (ISUG) which will share vital strategic, operational and tactical information and intelligence among the banking community using an automated platform; and create a trusted community where LFIs will meet to discuss cybersecurity threats and share related information, intelligence and best practices.

12.7.4 The core objectives of the ISUG are to protect the financial system by preventing, detecting and responding to cyber-attacks; to facilitate the sharing of information, intelligence and best practices between financial infrastructures; and to raise awareness of cybersecurity threats.

12.7.5 LFIs should establish a process to detect and respond to misinformation related to the LFI that are propagated via the Internet. The LFI should consider engaging external media monitoring services to facilitate the evaluation and identification of online misinformation.

12.8 *Regulatory Reporting Requirements*

12.8.1 Within 24 hours of becoming aware of a cyber-incident, an LFI shall alert the ECCB and the LFIs ISUG, that a cyber-incident occurred. The compromised LFI should complete the incident report provided in Appendix I and submit to the ECCB within 48 hours of the incident.

12.8.2 LFIs should engage in trusted information sharing with the banking community through the LFIs ISUG and the ECCU Bankers Association after a security breach. Technical information such as the threat actors, vulnerabilities exploited, and root cause analysis should be shared as soon as it is available. The information shared should include the following:

- A brief summary of the cyber threat or incident and lessons learnt;
- Sources and key contact of the information provider;
- Campaign, attack pattern investigated;

- Exploited vulnerabilities already fixed or still emerging;
- Threat actors or suspected attackers, if known, and root cause analysis;
- Course of action already taken and planned; and
- Possible remedies and mitigations extracted from the precedent/ similar cases.

12.8.3 The ECCB reserves the right to engage in trusted information sharing with the banking community through the LFIs ISUG and the ECCU Bankers Association after a security breach has been reported by an LFI. Technical information such as the threat actors, vulnerabilities exploited, and root cause analysis will be shared as soon as it is available.

12.8.4 An LFI shall provide an update on the incident to the ECCB; as per a frequency determined by the ECCB. The update(s) will continue until the incident is deemed resolved by the ECCB.

12.8.5 Following the resolution of the cyber-incident, an LFI shall conduct a post-incident review and submit same to the ECCB. The review should at a minimum include lessons learnt and a plan of action to address identified deficiencies and IT controls.

12.9 *Cyber Liability Insurance*

As the number of applications, devices, and information systems increases, LFIs become more vulnerable to attacks resulting in the need for insurance coverage for cyber risks similar to coverage against business problems, natural disasters, and physical risks.

Cyber liability insurance is structured to transfer indemnifiable first and third party losses. The first party losses include the cost of crisis management, customer notification, network business interruption and associated direct cost, systems recovery, and reconstitution of damaged software and digital assets. Third party losses are those costs experienced by third-parties and include liability for security

breaches and data privacy in general, defense costs, failing to defend against a cyber-attack, investigation costs and, potentially, penalties and fines.

12.9.1 LFIs should consider the purchase of cyber liability insurance or transferring its operational risk to an insured third-party service provider as part of the risk transfer and mitigation strategy.

12.9.2 LFIs should be mindful that cyber liability insurance policies typically do not cover indirect costs from cyber-attacks that manifest over the medium to long-term such as reputational damage, lost value of customer relationship, increased funding costs and insurance premiums, and the cost of having to boost defense systems post breach to increase resilience against cyber risk.

12.9.3 LFIs should be cognizant of the fact that despite the benefits of cyber liability insurance as a risk transfer strategy, it is by no means a replacement or substitute for active cyber risk management.

12.10 *Cyber-Attack Exercises*

12.10.1 The LFI 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 [18], table-top [19], cyber range [20] or adversarial attack simulation[21] exercises.

12.10.2 Based on the type and objectives of the exercise, the LFI 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.

12.10.3 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 LFI's production systems, the exercise must be closely supervised and performed in a controlled environment.

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

[18] Social engineering is a process in which cyber criminals manipulate an unsuspecting person into divulging sensitive details such as passwords through the use of techniques such as phishing, identity theft and spam.

[19] 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.
September 2006.

[20] 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.

[21] Adversarial attack simulation exercise provides a more realistic picture of an FI'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 FI's critical business functions or services.

13 Management of IT Outsourcing Risks

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 locally or abroad.

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

a) LFIs 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.
b) All parties concerned, including those from the service provider, should receive regular training in activating the contingency plan and executing recovery procedures.
c) LFIs should have contingency plans in place based on credible worst-case scenarios for service disruptions to prepare for the possibility that their current 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.

13.1 *Cloud Computing*

13.1.1 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.

13.1.2 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 set of guidelines when subscribing to CS.

13.1.3 LFIs 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, LFIs 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.

13.1.4 LFIs 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.

14 Internet of Things

a) 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 LFI's network or the Internet. Privacy of end-users IoT device can no longer be seen as an add-on to existing products or services. As with all information assets, the LFI should maintain an inventory of all its IoT devices, including information such as the networks which they are connected to and their physical locations.

b) 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 LFI's network and systems or as a launch pad for cyber-attacks on the LFI. Compromised IoT devices may additionally exfiltrate data and cause

disruption of the network during such orchestrated attacks. The LFI should assess and implement processes and controls to mitigate risks arising from IoT.

c) 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 LFI's network and launching malware or DoS attacks. To further reduce IoT risks, the LFI should host IoT devices in a separate network segment from the network that hosts the LFI's information systems and confidential data.
d) The LFI should implement controls to prevent unauthorised access to IoT devices. In light of privacy risks that the use of IoT technology brings, LFI's should take additional measure to safeguard Personally Identifiable Information.
e) Similar to other information systems, the LFI should monitor IoT devices for suspicious or anomalous system activities so that prompt actions can be taken to isolate compromised devices.
f) Regulatory aspects of collected IoT data should be taken in to consideration such as General Data Protection Regulation (GDPR), and Clarifying Lawful Overseas Use of Data (CLOUD) act.
g) With new and emerging technology, it is critical that proper risk assessment, due diligence and due care be taken into consideration. Among the developing technologies to be monitored for technology risks are the application and use of artificial intelligence, machine learning and quantum computing.

Appendix I: Cyber-Incident Report

Instructions:

Within 48 hours of a suspected or confirmed cyber-incident complete this form and submit to the ECCB.

Section (A)	
Particulars:	
1. Licensed Financial Institution	
2. Date and time of notification	
3. Name of Reporting Officer	
4. Designation/Department	
5. Contact details (e.g. email, mobile)	
Details of Incident:	
1. Discovery date and time of incident	
2. Nature of incident(s)	
3. Affected area(s)	
4. What actions or responses have been taken?	
Impact Assessment(examples are given but not exhaustive):	
1. Business impact including availability of services – Treasury Services, Cash Management, Branches, ATMs, Internet Banking, Mobile Banking, Clearing and Settlement activities etc.	
2. Stakeholders' impact – affected retail/corporate customers, affected participants including operator, settlement institution and service providers etc.	
3. Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds etc.	
4. Reputational impact and Compliance risk	
5. Regulatory and Legal impact	
Section (B)	
Detailed chronological order of events:	
1. Date of incident, start time and duration.	
2. Escalation steps taken, including approvals sought for interim measures to mitigate the event, and reasons for taking such measures	

3. Stakeholders informed or involved	
4. Various channels of communications involved	
5. Rationale on the decision/activation of BCP and/or IT DR	
Detailed Root Cause Analysis:	
1. Factors that caused the problem/ Reasons for occurring	
2. Interim measures to mitigate/resolve the issue, and reasons for taking such measures, and	
3. Steps identified or to be taken to address the problem in the longer term.	
Final assessment and remediation:	
1. Conclusion on cause and effects of incident	
2. List the corrective actions taken to prevent future occurrences of similar types of incident	
3. Target date of resolution_____ (DD/MM/YY).	

Appendix A – Guidelines sections mapping to leading Standards and Regulatory Guidelines

Section	Title	COBIT 2019 Processes	NIST CSF 1.1 Functions	ISO/IEC 27002 Controls	EBA/GL/2019/04 Sections	MAS TRM 2021 Sections
3	Oversight of Technology Risks by the Board and Senior Management					
3.1	Roles and Responsibilities	All	ID.GV	A.6.1	3.3.1	3.1
3.2	IT Policies, Standards and Procedures	All	ID.GV	A.5.1	3.3.1 3.4.1	3.2
3.3	People Selection Process	APO07	ID.AM	A.7.1	n/a	3.5
3.4	IT Security Awareness	DSS05	PR.AT	A.7.2	3.4.7	3.6
4	Technology Risk Management Framework					
4.1	Information System Assets	APO01	ID.AM	A.8.1	3.3.2	3.3
4.2	Risk Identification	APO12	ID.RA	(ISO 27005)	3.3.3	4.2
4.3	Risk Assessment	APO12	ID.RA	(ISO 27005)	3.3.3	4.3
4.4	Risk Treatment	APO12	ID.RA	(ISO 27005)	3.3.4; 3.3.5	4.4
4.5	Risk Monitoring and Reporting	APO12	ID.GV; ID.RA	(ISO 27005)	3.3.4	4.5
5	Operational IT Risk Guidelines					
5.1	IT Project Management	BAI11	n/a	A.6.1	3.6.1	5.1; 5.2
5.2	System Security Requirements and Testing	BAI02	n/a	A.14.2	3.4.6	5.5; 5.7
5.3	End User Development	n/a	n/a	n/a	n/a	6.5
5.4	IT Audit	MEA04	n/a	A.12.7	3.3.6	15.1
5.5	Audit Planning and Remediation Tracking	MEA04	n/a	A.12.7	3.3.6	15.1
6	IT Service Management					
6.1	Change Management	BAI06	PR.IP	A.12.1; A14.1; A.14.2	3.6.3	7.5
6.2	Program Migration	BAI07	n/a	n/a	n/a	n/a
6.3	User Access Management	DSS05	PR.AC	A.9.1; A.9.2; A.9.4	3.4.2	9.1
6.4	Privileged Access Management	DSS05	PR.AC	A.9.1; A.9.2; A.9.4	3.4.2	9.2
6.5	Remote Access Management	DSS05	PR.AC	A.9.1	n/a	9.3
6.6	Incident Management	DSS02	PR.IP; RS.AN; RS.MI	A.16.1	3.5.1	7.7
6.7	Problem Management	DSS03	n/a	n/a	3.5.1	7.8
7	Operational Infrastructure Security Management					
7.1	Data Loss Prevention	DSS05	n/a	n/a	3.4.4	11.1
7.2	Technology Refresh Management	BAI06	n/a	n/a	n/a	7.3
7.3	Networks and Security Configuration Management	DSS05	PR.IP; PR.AC; DE.CM	A.13.1	3.4.4	11.2
7.4	Vulnerability Assessment and Penetration Testing	DSS05	ID.RA; PR.IP; DE.CM; RS.AN; RS.MI	A.12.6	3.4.4	13.1; 13.2
7.5	Patch Management	DSS01; DSS05	RS.MI	A.12.2	3.4.4	7.4
7.6	Security Monitoring and Detection	DSS05	All DE	A.12.4	3.4.5	12.2
8	Online Financial Services					
8.1	Online Systems Security	n/a	n/a	n/a	n/a	14.1
8.2	Mobile Online Services and Payments Security	n/a	n/a	n/a	n/a	14.1
8.3	Bank specific: Payment Card Security (ATM's, Credit and Debit Cards)	n/a	n/a	n/a	n/a	n/a
8.4	Banks specific: Payment Card Fraud	n/a	n/a	n/a	n/a	14.3
8.5	Bank: ATMs and Payment Kiosks Security	n/a	n/a	n/a	n/a	n/a
9	Systems Reliability, Availability and Recoverability					
9.1	Systems Availability	DSS04	PR.DS	A.17.1	3.7	8.1
9.2	Data Backup Management	APO14	PR.IP	A.12.3	3.5	8.4
9.3	Disaster Recovery Plan	DSS04	PR.IP	A.17.1	3.7.1; 3.7.2; 3.7.3	8.2
9.4	Disaster Recovery Testing	DSS04	PR.IP	A.17.1	3.7.4	8.3
9.5	Data Center protection	DSS01; DSS04	ID.AM; PR.AC; PR.AT; PR.IP; DE.CM	A.11.1	3.4.3	8.5
9.6	Data Center Resiliency	DSS01; DSS04	ID.BE	A.17.2	3.7	8.5
9.7	Cyber-Attack Exercises	n/a	n/a	n/a	n/a	13.3; 13.4; 13.5
10	Management of IT Outsourcing Risks	APO08; APO09; APO10	ID.SC	A.15.1; A.15.2	3.2.3	3.4
10.1	Cloud Computing	n/a	n/a	n/a	n/a	11.1
11	Internet of Things	n/a	n/a	n/a	n/a	11.5

Legend – Coverage Mapping

- Fully (equal or higher than 85%)
- Largely (between 85% and 50%)
- Partially (between 15% and 50%)
- Not (less than 15%)

n/a No specific topic in the target