30th January, 2025

FINANCIAL SERVICES COMMISSION

TECHNOLOGY AND CYBER RISK MANAGEMENT GUIDELINE

FINANCIAL SERVICES COMMISSION

Technology and Cyber Risk Management Guideline

This Guideline was issued on December 1st, 2024 pursuant to Section 53 of the Financial Services Commission Act, 2010-10

Table of Contents

Purpose and Scope

This guideline establishes the Financial Services Commission's (the "Commission") regarding technology and cyber risk management. It applies to all financial institutions (FIs) the Commission regulates and aims to develop greater resilience to technology and cyber risks.

The extent and degree to which FIs implement this guideline should be proportional to the level of risk and complexity of the services offered and the technologies supporting such services.

This guideline is effective December 01st 2024

1. Glossary of Terms

Adversarial Attack Simulation Exercise Planned cyber security assessments that simulate attacks against people, processes and technology underpinning a company's critical business functions or services.
Biometric Technologies The use of technology to identify a person based on some aspect of their biology such as voice patterns and facial recognition.
Bring Your Own Device (BYOD) A policy that allows employees in a company to use their personal devices, such as laptops and tablets, to access work-related systems, such as corporate emails and other software applications.
Cyber Event An actual or suspected unauthorized system access that aims to control a company's online servers through various techniques.
Cyber Incident A breach of a company's system security policy through methods such as social engineering, man-in-the-middle attacks, and denial of service attacks.
Cyber-range An interactive, simulated representation of a company's system that is connected to a simulated internet environment to facilitate the training of potential cybersecurity professionals.
Cybersecurity Risk The potential adverse impact on a company's operations through unauthorized access to its IT systems, which can result in the possibility of failure, disruption, modification, or destruction of the company's IT systems and/or the data contained therein.
Data Confidentiality The protection of sensitive or confidential data such as customer details from unauthorized access and disclosure.
Data Loss Prevention (DLP) Data loss prevention- sometimes called data leak prevention or information loss prevention- is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data. It can help your organization monitor and protect sensitive information across on-premises systems, cloud-based locations, and endpoint devices.

Denial of Service (DoS) A type of cyber-attack aimed at preventing an authorized user from accessing resources such as networks, websites, or other online services.
Domain name system hijacking (DNS) A cyber-attack technique where a cyber-criminal redirects authorized users to malicious sites.
Endpoint Detection and Response (EDR) Software designed to automatically protect an organization's end users, endpoint devices, and IT assets against cyber threats that get past antivirus software and other traditional endpoint security tools.
Fraudulent Online transactions The unauthorized use of an individual's confidential information to conduct transactions or payments via the Internet.
General-purpose device A device such as a desktop computer, laptop, or mobile device, designed to install software applications.
Hardware The physical aspects of a computer or a related device such as a keyboard, printer, motherboard etc.
Information/Technology Asset The hardware and software within a company's IT environment that supports the provision of its technological services.
Least Privilege A principle where access rights and system privileges are granted based on job responsibility.
Man-in-the-middle attack (MITMA) A type of cyber-attack where cyber criminals secretly intercepts and transmit messages between an authorized user and an application to steal personal information such as account details, credit card numbers etc.
Multi-factor Authentication (MFA) An authentication method that requires an authorized user to provide two or more verification factors to gain access to a company's resources such as online banking.
Online Financial Services

A mechanism that allows authorized users to conduct financial transactions such as online banking and online trading via the Internet.
Segregation of duties A principle that divides crucial IT functions among the different staff members to ensure that no one individual has enough information or access privileges to execute damaging fraud.
Social Engineering A process where cyber criminals manipulate innocent persons into disclosing confidential information such as passwords and banking information.
Software The applications and programs used to operate and execute tasks on computers and other related devices.
System Development life cycle (SDLC) SDLC is a process that provides a framework for executing a company's system. Its seven steps include planning, system analysis and requirements, system design, development, integrating and testing, implementation, and operations and maintenance.
System Testing A method used to validate the software specifications through the evaluation of corresponding requirements.
Table-top Exercise A discussion-based exercise where the participants of a simulated emergency scenario meet to validate the content of the scenario.
Technology Risk A type of business risk related to the malfunctioning or disruption of a company's IT functions as it relates to the people or processes that enable and support the company's needs and can result in financial loss.

2. Technology and Cyber Risk Management- Governance and Oversight

(A) Role of the Board of Directors and Senior Management

(1) The board of directors and senior management of FIs should ensure that:

a. The tone is set from the top and a strong culture of technology risk awareness and management is cultivated at all levels of staff within the FI.

b. Effective internal controls and risk management practices are implemented to achieve security, reliability and resilience of its Information Technology (IT) operating environment.

c. A Chief Information Officer, Chief Technology Officer or Head of IT and a Chief Information Security Officer or Head of Information Security with the relevant skill set and experience are appointed. The Chief Executive Officer should minimally approve the appointments.

d. The appointed person referred to in point (c) above, should at a minimum:
   i. Implement and oversee the FIs cyber security program.
   ii. Manage and monitor Incident Response Activities.
   iii. Promote a robust information security culture within the FI.
   iv. Oversee the FI's IT & Cybersecurity personnel and ensure adequate training and awareness of the general staff complement.

e. A technology and cyber risk management strategy is established and implemented.

f. Key IT decisions are made in accordance with the FI's risk tolerance.

(2) The board of directors or a committee delegated by it should:

a. Ensure that a sound and robust risk management framework is established and maintained to manage technology and cyber risks.

b. Ensure that there is a technology and cyber risk management function such as a Risk Officer to govern the technology and cyber risk management framework and strategy, as well as to provide an independent view of the technology and cyber risks faced by the FI.

c. Provide senior executives who are responsible for executing the FI's technology and cyber risk management strategy with sufficient authority, resources and access to the board of directors.

d. Approve the risk tolerance statement that expresses the nature and extent of technology and cyber risks that the FI is willing and able to assume.

e. Undertake regular periodic reviews of the technology and cyber risk management strategy for continued relevance.

f. Assess management competencies for managing technology and cyber risk; and

g. Establish an independent audit function to assess the effectiveness of controls, risk management and governance of the FI and report to the Board.

(3) Senior management is required to:

a. Establish the technology and cyber risk management framework and strategy.

b. Manage technology and cyber risks based on the established framework and strategy.

c. Ensure sound and prudent policies, standards and procedures for managing technology and cyber risks are established and maintained and that standards and procedures are implemented effectively.

d. Appoint a Risk Officer with the relevant skillset and experience. The role of the risk officer may be carried out by a function or a group of functions within the FI, who should be authorized to manage technology and cyber security risks.

e. Ensure the roles and responsibilities of staff are outlined clearly in managing technology and cyber risks; and

f. Notify the board of directors of significant and adverse technology and cyber risk developments and incidents that are likely to have a substantial impact on the FI and its customers.

(B) The Establishment of Standard Operating Procedures (SOPs)

(1) An FI should establish SOPs and, where applicable, incorporate industry standards and best practices to manage technology risks and safeguard information assets in the FI.

(2) The SOPs should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape.

(3) The FI should review and assess risks associated with deviations thoroughly. The risk assessment should be approved by senior management, and approved deviations should be reviewed periodically to ensure that residual risks remain at an acceptable level.

(4) Compliance processes should be implemented to verify that SOPs are observed. These include follow-up processes for non-compliance.

(C) Information Asset Management

(1) To have an accurate and complete view of its IT operating environment, an FI should establish information asset management practices that include the following:

a. Identification of information assets that support the FI's business and delivery of its services.

b. Classification of an information asset based on its security classification or criticality.

c. Ownership of information assets, and the roles and responsibilities of the staff managing the information assets; and

d. Establishment of SOPs to manage information assets according to their security classification or criticality.

(2) An FI should maintain a log of its information assets. The log should be reviewed regularly and updated whenever there are changes to the quantity of information assets.

(D) Outsourcing

(1) An FI should assess and manage its exposure to technology and cyber risks that may affect the confidentiality, integrity and availability of its IT systems and data at a third party prior to entering into a contractual agreement or partnership.

(2) On an ongoing basis, the FI should ensure the third-party service provider employs a high standard of care and diligence in protecting data confidentiality and integrity as well as ensuring system resilience.

(3) Sub-outsourcing refers to a situation where an FI's service provider under an outsourcing arrangement further transfers a process, service or activity (or parts thereof) to another service provider. In this instance FIs should conduct rigorous due diligence to ensure compliance with regulatory requirements and the FI's IT security policy.

(E) Competency of Staff and other Personnel

(1) The FI should ensure all staff, including contractors and service providers, have the requisite competence and skills to perform their IT functions and manage technology and cyber risks.

(2) A background check on all personnel who have access to the FI's data and IT systems should be performed to minimize insider threat.

(3) The FI should ensure that members of staff, vendors and contractors authorized to access their systems are also in compliance with their information system security policy.

(F) IT Security Awareness and Training

(1) A comprehensive IT security awareness training program should be established to maintain a high level of awareness among all staff in the FI. The content of the training program should at a minimum include information on the current cyber threat environment and its implications, the FI's SOPs, as well as an individual's responsibility to safeguard information assets.

(2) All management and staff of the FI should be aware of the applicable laws, regulations, and guidelines pertaining to the use of, and access to, information assets.

(3) A training program should be undertaken annually for all staff, contractors and service providers who have access to the FI's information assets.

(4) The board of directors should undergo training to raise their awareness of risks associated with the use of technology and enhance their understanding of technology and cyber risk management practices.

(5) The training program should be reviewed regularly to ensure its contents remain current and relevant. The review should take into consideration changes in the FI's IT security policies, current and emerging risks, and the evolving cyber threat environment.

3. Risk Management Framework- Technology and Cyber Security

(A) Risk Management Framework

(1) An FI should establish a risk management framework to manage technology and cyber risks. Appropriate governance structures and processes should be established, with well-defined roles, responsibilities and clear reporting lines across the various organisational functions.

(2) Effective risk management practices and internal controls should be incorporated to achieve data confidentiality and integrity, system security and reliability as well as stability and resilience in its IT operating environment.

(3) A risk officer, who is accountable for ensuring proper risk treatment measures are implemented and enforced for specific technology and cyber risks, should be identified.

(B) Components of the Technology and Cyber Risk Management Framework

i. Technology and Cyber Risk Identification

An FI should:

a. Establish a process to conduct regular vulnerability assessment (VA) on their IT systems to identify security vulnerabilities and ensure risk arising from these gaps are addressed in a timely manner.

b. Identify any threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third-party service providers.

c. Perform a VA which should at a minimum include vulnerability discovery, identification of weak security configurations and open network ports as well as application vulnerabilities. For web-based systems, the scope of VA should include checks on common web-based vulnerabilities.

ii. Technology and Cyber Risk Penetration Testing (PT)

a. An FI should carry out PT after a VA has been conducted to obtain an in-depth evaluation of its technology and cyber security defenses.

b. PT should be conducted on an FI's production environment to obtain a more accurate assessment of the robustness of their security measures.

c. The frequency of PT should be determined based on factors such as system criticality and the system's exposure to technology and cyber risk. The FI is expected to conduct PT annually to validate the adequacy of the security controls for systems that are directly accessible from the internet.

iii. Technology and Cyber Risk Assessment

a. An FI should perform an analysis of the potential impact and consequences of the threats and vulnerabilities on the overall business and operations. When assessing technology and cyber risks, consideration should be given to financial, operational, legal, reputational, and regulatory factors.

b. To facilitate the prioritisation of technology risks, a set of criteria measuring and determining the likelihood and impact of the risk scenarios should be established.

iv. Technology and Cyber Threat Exercises

a. An FI should undertake regular scenario-based technology and cyber threat exercises to validate its response and recovery to prevalent and emerging threats. These exercises can include social engineering, table-top or cyber range exercises.

b. Subject to the exercise objectives, an FI is expected to involve the relevant stakeholders, including the Commission, senior management, business functions, corporate communications, crisis management team, service providers and technical staff responsible for technology and cyber threat detection, response and recovery.

v. Technology and Cyber Risk Adversarial Attack Simulation Exercise

a. To test and validate the effectiveness of its technology and cyber defense and response plan against popular technology and cyber threats, an FI should perform an adversarial attack simulation exercise.

b. The objectives, scope and rules of engagement should be defined before the initiation of the exercise, and the exercise should be conducted in a controlled manner under close supervision to ensure the activities undertaken by the testing team are not detrimental to the FI's production systems.

c. An FI should design the exercise scenario by using threat intelligence relevant to their IT environment to identify threat actors who are most likely to pose a threat to the FI and identify tactics, techniques and procedures most likely to be used in such attacks.

vi. Technology and Cyber Risk Remediation Management

a. A comprehensive remediation process should be established to track and resolve issues identified from the technology and cyber security assessments or exercises. The process should minimally include the following:

   i. Severity assessment and classification of an issue
   ii. Timeframe to remediate issues of different severity; and
   iii. Risk assessment and mitigation strategies to manage deviation from the framework.

b. A technology and cyber incident response and management plan should be established to swiftly isolate and neutralise the threat and securely resume affected services.

c. Information from cyber intelligence and lessons learnt from the technology and cyber incidents should be used to enhance the existing controls or improve the technology and cyber incident management plan.

d. An FI should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance. The IT control and risk mitigation approach should be subject to regular review and update, considering the changing threat landscape and variations in the FI's risk profile.

e. An FI should assess whether risks have been reduced to an acceptable level after applying the mitigating measures as there are residual risks from threats and vulnerabilities which cannot be fully eliminated. The criteria and approving authorities for risk acceptance should be clearly defined and it should be correspondent with the FI's risk tolerance.

f. An FI should obtain insurance coverage for various insurable technology and potential cyber risks to reduce the financial impact such as recovery and restitution costs.

vii. Technology and Cyber Risk Monitoring, Review and Reporting

To facilitate continuous monitoring, prompt detection and response to technology and cyber incidents, an FI should:

a. Establish a security operations centre or acquire managed security services.

b. Define SOPs for security operations.

c. Establish a process to collect, process, review and retain system logs to facilitate the FI's security monitoring operations. The logs should be protected against unauthorised access.

d. Facilitate the identification of anomalies by establishing a baseline profile of each IT system's routine activities and analysing the system activities against the baseline profiles. The profiles should be regularly reviewed and updated.

e. Ensure timely escalation to relevant stakeholders regarding suspicious or anomalous system activities or user behavior.

f. Maintain a risk record to facilitate the monitoring and reporting of technology and cyber risks. Significant risks should be monitored closely and reported to the board of directors and senior management. The frequency of monitoring and reporting should be correspondent with the level of risk.

g. Develop technology risk metrics to highlight information assets that have the highest risk exposure to facilitate risk reporting to management. In determining the technology risk metrics, the FI should consider risk events and audit observations, as well as applicable regulatory requirements by the Commission.

viii. Technology and Cyber Risk Intelligence and Information Sharing

FIs should actively participate in IT & Cyber-Risk information sharing seminars with trusted parties to enable them to identify, assess, monitor, and respond to cyber threats. To maintain good cyber awareness, the FI should:

a. Establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the FI's operations and IT environment.

b. Obtain cyber intelligence monitoring services.

c. Establish a process to detect and respond to misinformation related to the FI via various communication networks.

4. Management of Technology Services

(A) Project Management Framework

(1) A project management framework should be established to ensure:

a. Consistency in project management practices, and delivery of outcomes that meet project objectives and requirements.

b. Policies, standards, procedures, processes, and activities are included to manage projects from initiation to closure.

c. Detailed IT project plans are established for all IT projects. An IT project plan should set out the scope of the project, as well as the activities, milestones and deliverables to be realised at each phase of the project. The roles and responsibilities of staff involved in the project should be clearly defined in the plan.

d. A risk management process is established to identify, assess, treat and monitor the associated risks throughout the project life cycle.

(2) A project committee consisting of key stakeholders, including the FI's shareholders and IT should be formed to provide guidance and oversight for large and complex projects that impact the operations of the business. This is to ensure milestones are reached and deliverables are realised in a timely manner.

(3) Risks and issues for large and complex projects, which cannot be resolved at the project management level should be escalated to the project committee and senior management.

(B) System Acquisition

(1) SOPs should be established to ensure selected vendors are competent to meet project requirements and deliverables.

(2) The level of assessment and due diligence performed should be correspondent with the criticality of the project deliverables to the FI.

(3) Vendor access to the FI's IT systems should be controlled and monitored. The FI should ensure rigorous security practices are in place to safeguard any sensitive data that is accessible to the vendor for the duration of the project.

(C) System Development Life Cycle (SDLC)

(1) SOPs for the various phases of the SDLC should be maintained. The framework should clearly define the processes, procedures, and controls in each phase of the life cycle,

such as initiation/planning, requirements analysis, design, implementation, testing and acceptance.

(2) In order to minimise system vulnerabilities, security should be incorporated within each phase of the SDLC. An FI should include security specifications in the system design, perform continuous security evaluation and adhere to security practices throughout the SDLC.

(3) Security requirements should minimally cover key control areas such as access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling.

(4) The SDLC should, where relevant, involve the IT security function in each phase of the life cycle.

(D) System Requirements Analysis

(1) Functional requirements for the IT system should be identified, defined, and documented. An FI should also establish and document key requirements such as system performance, resilience, and security controls.

(2) An FI should assess potential threats and risks regarding the IT system and determine the acceptable level of security required to meet its business operational needs.

(E) System Design and Implementation

(1) During the design phase an FI should:

a. Review the proposed layout and design of the IT system, including the IT controls to be built into the system, to ensure they meet the defined requirements, before implementation.

b. Verify that system requirements are met by the current system design and implementation. Any changes to, or deviations from, the defined requirements should be approved by the relevant stakeholders.

c. Engage the relevant domain experts to participate in the design review.

(F) System Testing

(1) An FI should:

a. Determine a process for system testing where the scope of testing should cover system function, security controls, business logic and system performance under various conditions. Prior to testing, a test plan should be established and approved.

b. Maintain separate physical and logical environments for unit, system integration and user acceptance testing. Access to each environment should be restricted when necessary.

c. Perform regression testing for changes such as an enhancement to the existing IT system to verify that the system continues to function after the changes have been made.

d. Report major issues that could have an unfavorable impact on the FI's operations to the project committee. Issues identified by testing should also be addressed.

e. Ensure the results of all testing that was conducted are documented in the test report and signed by the relevant parties.

(G) Quality Assurance and Control

(1) An FI should define the expected quality traits and the assessment metrics for the project deliverables based on its quality control standards.

(2) An independent quality assurance function should be performed to ensure project activities and deliverables comply with the FI's SOPs.

(H) Technology Configuration and Refresh Management

(1) To effectively control the IT systems, an FI should:

a. Implement a configuration management process to ensure accurate information of its hardware and software is maintained.

b. Conduct regular reviews and verify the configuration information of its hardware and software is accurate.

c. Avoid using outdated and unsupported hardware or software.

d. Develop a technology refresh plan for the replacement of hardware and software before they expire.

e. Conduct a risk assessment for hardware and software approaching the expiry date to evaluate the risks of their continued use. Effective risk mitigation measures should also be implemented.

(I) Patch Management

(1) A patch management process should be implemented to ensure the timely application of patches across FI's IT systems to correct any software errors.

(2) Patches should be tested before being deployed to the production environment.

(J) Change and Release Management

(1) An FI should:

a. Establish and implement a technology change and release management process to ensure changes to information assets are assessed, tested, reviewed, and approved before deployed.

b. Segregate duties in the change management process to prohibit one individual from developing, compiling, and moving software codes from one environment to another.

c. Perform a backup of the information asset before implementing the change and establish a rollback plan to revert the information asset to its previous state if a problem arises during the process.

d. Implement controls to maintain traceability and integrity for all software codes that are moved between production and non-production IT environments.

(K) Incident and Problem Management

(1) The occurrence of an IT incident may result in the disruption, malfunction or error on an FI's server, network or end point which can impact its operations and service delivery. FIs should appropriately manage such incidents to understand root causes and appropriate preventative measures to reduce prolonged disruption of IT services or further aggravation.

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

(3) FIs should establish corresponding escalation and resolution procedures where the resolution timeframe is proportionate with the severity level of the incident. The predetermined escalation and response plan for IT security incidents should be tested on a regular basis.

(4) An FI should establish an incident and problem management framework to restore affected IT services or systems to a secure and stable condition to ensure minimal impact to business operations.

(5) The incident and problem management framework should minimally cover:

a. SOPs for handling IT incidents or problems

b. Maintenance and protection of supporting evidence for the investigation and diagnosis of incidents; and
c. The roles and responsibilities of staff and external parties involved in the process.

(6) An FI should maintain a log of past incidents which should include previous lessons learnt to facilitate the diagnosis and resolution of future incidents with similar characteristics.

5. Technology Resilience

(A) System Availability

(1) An FI should ensure that their IT systems are designed to achieve the level of system availability that is proportionate to its operational needs. Notwithstanding such, FIs should also establish SOPs to respond to situations when pre-defined thresholds for system resources and system performance have been breached.

(2) It is vital for FIs to conduct regular system reviews and testing to ensure a robust level of resilience exists to facilitate sustainable business operations. At a minimum, the review should include a mapping of internal and external dependencies of the FI's IT systems to determine any single point of failure.

(B) Disaster Recovery

(1) An FI should establish a disaster recovery framework inclusive of procedures to recover systems from various disaster scenarios and the roles and responsibilities of relevant personnel in the recovery process.

(2) The disaster recovery framework should be reviewed annually and updated when there are significant changes to business operations, information assets or environmental factors.

(3) An FI should perform regular testing of its disaster recovery plan to validate the effectiveness of the plan and ensure its systems are able to meet the recovery objectives.

(4) An FI should establish a data backup strategy and develop a plan to perform regular backups so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted.

6. Access Rights and System Privileges

(A) User Access Rights

(1) Access rights should be authorised and approved by appropriate parties, such as the owner of the information assets, which can be an FI and its shareholders. SOPs for user access management should be established to provide, change, and revoke access rights to information assets when necessary.

(2) Principles such as “segregation of duties” and “least privilege” should be applied when granting staff access to information assets to prohibit the access of one person to perform sensitive system functions.

(3) An FI should ensure a record of user access and user management activities are logged for audit and investigation purposes.

(4) To enforce solid password controls for users’ access to IT systems, an FI should establish a password policy and SOPs regarding same. At a minimum, the password policy should include minimum password length and history, password complexity and maximum validity period.

(5) In efforts to safeguard an FI's systems and data from unauthorised access, the FI should implement multi-factor authentication for users with access to sensitive system functions.

(6) A user access review should be regularly conducted to identify inactive and redundant user accounts, as well as inappropriate access rights. Any issues identified during the review should be promptly resolved.

(7) The same monitoring restrictions utilised for an FI's staff should be followed by service providers who have access to the FI's information assets.

(B) Privileged Access Rights

(1) Access to privileged accounts should only be granted on a need-to-use basis, where the activities of these accounts should be logged and reviewed as a component of an FI's ongoing monitoring process.

(2) A FI should establish SOPs to manage and monitor the use of system and service accounts for suspicious or unauthorised activities.

(C) Remote Access Rights

(1) Remote access allows users to connect to the FI's internal network via an external network to access the FI's data and systems, such as emails and business applications.

(2) Remote access infrastructure should be thoroughly tested for vulnerabilities. When utilising cloud infrastructure, the FI should review existing controls and conduct security assessment and testing.

(3) To safeguard against unauthorised access to the FI's IT environment, multi-factor authentication should be implemented, when possible, for users utilising remote access. Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping.

(4) An FI should ensure remote access to their information assets is only allowed from devices that have been secured according to their security standards.

7. Data and Infrastructure Security

(A) Data Security

(1) An FI should:

a. Develop SOPs to detect and prevent unauthorised access, modification, copying or transmission of confidential data.

b. Implement Data Loss Prevention (DLP), as well as unauthorised modification in systems and endpoint devices.

c. Ensure systems managed by the FI's service providers have the same level of protection and ensure they are subjected to the same security standards.

d. Implement security measures to prevent and detect the use of unauthorised internet services which allow users to communicate or store confidential data.

e. Ensure written approval is obtained from senior management in exceptional situations when sensitive production data needs to be used in non-production environments.

f. Implement SOPs in non-production environments to manage the access and removal of data to prevent data leakage.

g. Permanently delete confidential data from storage media, systems and endpoint devices before they are disposed of or redeployed.

(B) Network Security

(1) An FI should:

a. Secure the network between the FI and the internet, as well as connections with third parties by installing network security devices such as firewalls.

b. Deploy effective security mechanisms to protect information assets to minimise the risk of cyber threats, such as insider threats.

c. Detect and block malicious network traffic by deploying network intrusion detection and prevention systems in the FI's network.

d. Prevent unauthorised devices from connecting to its network by implementing network access controls.

e. Review access control rules in network devices such as firewalls, routers, switches, and access points on a regular basis to ensure they are kept up to date.

f. Promptly remove outdated rules and insecure network protocols as these can be manipulated to gain unauthorised access to the FI's network and systems.

g. Implement an effective Denial of Service (DoS) protection to detect and respond to various types of DoS attacks.

h. Engage DoS mitigation service providers to filter potential DoS traffic before it reaches the FI's network infrastructure.

i. Regularly conduct a review of the FI's network architecture, including the network security design, as well as system and network interconnections to identify potential cyber security vulnerabilities.

(C) System Security

(1) An FI should:

a. Outline the security standards for their hardware and software configurations that will minimise their exposure to cyber threats. The standards should be reviewed periodically for relevance and effectiveness.

b. Establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely manner.

c. Implement End Point Detection and Response (EDR) software which will regularly scans and monitors systems for malicious files or anomalous activities.

d. Implement security measures, such as application whitelisting to ensure only authorised software is allowed to be installed on the FI's systems.

e. Conduct a comprehensive risk assessment and ensure appropriate measures are implemented to secure its Bring Your Own Device (BYOD) environment before allowing staff to use their personal device to access the corporate network.

(D) Electronic Information Assets

(1) Electronic information assets refer to devices such as smartphones, multi-function printers and security cameras which can be connected to an FI's network or the internet. An FI should:

a. Maintain a record of all its electronic devices, including information such as the networks which they are connected to and their physical locations.

b. Implement controls to prevent unauthorised access to their devices.

c. Implement SOPs to mitigate risks arising from electronic devices, since most of these devices are designed with minimal security controls.

d. Monitor their electronic devices for suspicious or anomalous system activities so that compromised devices can be promptly isolated.

e. Host electronic devices in a separate secured network segment from the network that hosts the FI's systems and confidential data to prevent a cyber threat actor from accessing the FI's network.

8. Online Financial Services

(A) Secure Online Financial Services

(1) When delivering online financial services, an FI should:

a. Implement security and control measures which are proportionate with the risk involved to ensure the security of data and online services.

b. Secure its communications channels to protect customer data. This can be achieved through data encryption and digital signatures.

c. Take adequate measures to minimize their exposure of online financial services to common attack vectors such as man-in-the-middle attack (MITMA), domain name system (DNS) hijacking and distributed denial of service (DDoS)attacks.

d. Implement specific measures aimed at addressing the risks of mobile applications if the online financial services are accessible via a mobile device.

e. Make mobile applications or software available to customers through official mobile application stores, or other secure delivery channels.

f. Actively monitor for phishing campaigns targeting the FI and its customers. Immediate action should be taken to report phishing attempts to service providers to facilitate the removal of malicious content.

g. Alert its customers of such campaigns and advise them of security measures to adopt to protect against phishing.

(B) Automated Teller Machines (ATMs) and Payment Card Security (Credit and Debit Cards)

(1) To facilitate consumer protection and enforce consumers' confidence regarding the use of ATMs, the FI should at a minimum:

a. Conduct video surveillance of activities at the machines utilising quality CCTV systems.

b. Install anti-skimming solutions on the machines to detect the presence of foreign devices placed around the perimeter of the card entry slot.

c. Implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission.

d. Install detection mechanisms and send alerts to the FI to foster remediation management.

(2) FIs should also ensure mechanisms are in place to prevent debit and credit card fraud. When issuing cards, the FI should follow best practices to institute payment card security such as EMV chip technology and other technological enhancements.

(C) Customer Verification for Online Transactions

(1) To secure customer activity on the online environment, an FI should:

a. Utilise multi-factor authentication at login for online financial services to protect the customer verification process.

b. Safeguard the confidentiality of customer passwords by verifying them in a hardened or tamper-resistant system.

c. Protect the integrity of customer accounts' data and transaction details through the implementation of digital signatures to permit high-risk activities. High-risk activities include changes to the customer's mailing address, email address, high-value funds transfers and revision of funds transfer limits.

d. Implement suitable risk-based authentication that provides customers with verification options that are proportionate with the risk level of the transaction and sensitivity of the data.

e. Establish short and practicable validity periods when implementing time-based one-time passwords (OTPs), to lower the risk of a stolen OTP being used for fraudulent transactions.

f. Ensure biometric-related data and verification credentials are encrypted in storage where biometric technologies and customer passwords are used for customer verification.

g. Detect and terminate hijacked sessions to reduce the risk of an attacker maintaining a hijacked session indefinitely. Throughout the interaction with the customer, the FI should ensure the authenticated session, together with its encryption protocol, remains intact.

h. Perform a security risk assessment of alternate controls and processes, implemented for corporate customers to authorise transactions, to ensure they are proportionate with the risk of the activities undertaken.

(D) Fraudulent Online Transaction Management

(1) To detect and block suspicious or fraudulent online transactions, an FI should implement real-time fraud monitoring systems. SOPs should be established to investigate suspicious transactions or payments and to ensure issues are adequately and promptly addressed.

(2) FIs should inform customers of the security best practices that they should adopt when using online financial services. This includes measures to take to secure their electronic devices and identity information that is used to access online financial services.

(3) Customers should be alerted on a timely basis regarding new cyber threats so that they can take precautionary measures.

(4) FIs should advise their customers on the methods to detect unauthorised transactions and to promptly report security issues, suspicious activities or suspected fraud to the FI.

(5) FIs should also notify affected customers in writing of suspicious activities or funds transferred above a threshold that is defined by the FI or its customers.

9. IT Audit

(A) Audit Function

(1) FIs should:

a. Perform an audit to provide the board of directors and senior management with an independent and objective opinion of the adequacy and effectiveness of the FI's risk management, governance and internal controls relative to its existing and emerging technology and cyber security risks.

b. Identify a comprehensive set of auditable areas such as IT operations, functions and SOPs so that an effective risk assessment could be performed during audit planning.

c. Ensure the frequency of IT audits are proportionate with the criticality of, and risk posed by the IT information asset, function or process.

d. Ensure its IT auditors are competent to effectively assess and evaluate the adequacy of the IT SOPs and controls implemented.

10. Technology and Cyber Security Incident Reporting

(A) Criteria for Reporting to the Commission

(1) Reportable incidents (*see Appendix I)* may have one or more than one of the following characteristics:

a. Potential consequences to other FIs or the Barbadian financial system

b. Impact on the FI's systems affecting financial market settlement, confirmations or payments (e.g., Financial Market Infrastructure), or impact to payment services.

c. Impact to the FI's operations, infrastructure, data and/or systems, including but not limited to the confidentiality, integrity or availability of customer information.

d. Disruptions to business systems and/or operation, including but not limited to utility or data centre outages or loss or degradation of connectivity.

e. Operational impact to key/critical systems, infrastructure or data

f. Disaster recovery teams or plans have been activated, or a disaster declaration has been made by a third-party vendor that impacts the FI.

g. Operational impact to internal users, and that poses an impact to external customers or business operations.

h. The amount of impacted external customers is increasing; negative reputational impact is imminent (e.g., public and/or media disclosure)

i. Impact on a third party affecting the FI.

j. The FI's technology or cyber incident management team or protocols have been activated.

k. An incident has been reported to:

    i. A local government department

    ii. Other local or foreign supervisory or regulatory organisations or agencies

    iii. Any law enforcement agencies

    iv. Has invoked internal or external counsel.

l. An incident for which a cyber insurance claim has been initiated.

m. An incident assessed by an FI to be of a high or critical severity.

n. Technology or cyber security incidents that breach internal risk appetite or thresholds.

(2) For incidents that do not align with or contain the specific criteria listed above, or when an entity is uncertain, notification to the Commission is encouraged as a precaution.

(B) Notification Requirements

(1) FIs should inform the Commission within four (4) hours after an incident is classified, noting that an incident should be classified within the first twenty-four (24) hours of its detection. An incident is classified as major if it satisfies the requisite criteria in the Classification Matrix found in the *Instructions for the completion of the forms.*

(2) Cybersecurity events that have a reasonable likelihood of materially harming any part of the normal operation(s) of the FI, should also be reported via the Cyber Incident Reporting Forms to the Commission.

(3) Annually each FI should revise their Cybersecurity program where it has identified areas, systems or processes that require material improvement, updating or redesign. FIs 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 Commission.

(4) FIs 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.

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

(6) FIs should seek further guidance regarding the completion of the forms from *Instructions for the completion of the Major Cyber Incident Reporting Forms* which is accessible on the Commission's website.

(C) Failure to Report to the Commission

Failure to report incidents to the Commission as outlined above may result in increased supervisory oversight including but not limited to enhanced monitoring activities, watch-listing or staging of the FI pursuant to the Commission's ladder of intervention.