BANK OF MAURITIUS

Guideline on Cyber and Technology Risk Management

29 May 2023

(Page intentionally left blank)

Table of Contents

INTRODUCTION

Background

The outbreak of the pandemic has accelerated the digital transformation of the financial sector worldwide, including in Mauritius. While the Bank of Mauritius (Bank) fully supports this transformation, it acknowledges the related increase in the threat landscape and the potential spill over effects on financial stability. A sound and robust cyber and technology risk management framework is thus essential for the safety and soundness of financial institutions and for their resilience against such risks.

This guideline sets out the **minimum requirements** which banks and payment service providers are expected to implement with respect to cyber and technology risk management to ensure that the risks are well understood and managed appropriately.

In addition to the minimum requirements, banks and payment service providers shall consider implementation of encouraged measures set out in the guideline as well as standards in relevant international guidance documents, such as, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Control Objectives for Information and Related Technologies by ISACA and other relevant ISO standards as well as other best practices.

Banks and payment service providers shall implement a cyber and technology risk management framework commensurate with the size, nature and complexity of their activities, services and underlying technologies.

Other financial institutions shall refer to the requirements of the guideline and implement a cyber and technology risk management framework which is commensurate with their cyber and technology risk profile.

This guideline is largely based on the guidance on Cyber Resilience Oversight Expectations for financial market infrastructures issued by the European Central Bank in December 2018.

Authority

This guideline is issued under the authority of section 50 of the Bank of Mauritius Act 2004, section 100 of the Banking Act 2004 and section 17 of the National Payment Systems Act 2018.

Scope of application

This guideline applies to all financial institutions licensed or authorised by the Bank.

Effective date

This guideline shall come into effect on 29 May 2023.

Interpretation[1]

“administrative account” refers to any user account with full privileges and unrestricted access to:

(a) an operating system;
(b) a database;
(c) an application;
(d) a security appliance; or
(e) a network device.

“asset” refers to something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.

"black box testing" refers to a testing approach in which the tester is unaware of the environment.

“board” means the board of directors of a financial institution except for branches of foreign banks where ‘board’ means the local advisory board/committee. For branches of foreign banks with no local advisory board, the responsibilities assigned to the board shall rest on the Chief Executive Officer of the branch.

“control functions” mean those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance. This includes the risk management function, the compliance function and the internal audit function.

“critical systems, services, infrastructures and other assets” include systems, services, infrastructures and other assets whose failure will cause significant disruption to the operations of the financial institution and/or have a material impact on the safety and soundness and/or on the reputation of the financial institution. Financial institutions shall also take into consideration their ability to provide critical services and to comply with legal and regulatory obligations when assessing criticality of systems, services, infrastructures and other assets.

“cyber” refers to what is related to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

[1] Largely adapted from the Financial Stability Board’s Cyber Lexicon and the Guidance on cyber resilience for financial market infrastructures by the Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions.

"cyber and technology event" means any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.

"cyber and technology incident" means an event, whether resulting from malicious activity or not, which:

(a) adversely affects the security of an information system or the information the system processes, stores or transmits; or
(b) violates the security policies, security procedures or acceptable use policies.

Examples of cyber and technology incident would include the:

(i) data breaches such as unauthorised use, disclosure, modification, theft, loss, corruption or destruction of information;
(ii) interference with information technology (IT) operations;
(iii) interference with system operations;
(iv) denial of service; and
(v) distributed denial of service.

"cyber-attack" is the exploitation of a weakness with the intention of achieving an adverse effect on the information and communication technology environment.

"cyber-attacker" means a person carrying out a cyber-attack.

"Cyber and Technology Incident Response Plan" refers to the documented predetermined set of instructions or procedures to respond to and limit consequences of a cyber or technology incident.

"cyber and technology resilience" means the ability of a financial institution to continue to carry out its operation by anticipating and adapting to cyber or technology threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber and/or technology incidents.

"cyber and technology risk" means the combination of the probability of cyber and technology incidents occurring and their impact.

"cybersecurity" means protecting information, equipment, device, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction. This includes the 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 be involved.

"cyber threat" means a circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity.

“data breach” means a compromise of security that leads to the accidental, unauthorised, unlawful destruction, theft, loss, alteration, unauthorised use or disclosure of or access to data transmitted, stored or otherwise processed.

“defence-in-depth” refers to security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the financial institution.

“Denial of Service” means 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.

“designated sub-committee of the board” means the sub-committee of the board as designated under paragraphs 6 and 7 of the guideline.

“Distributed Denial of Service” means a denial of service that is carried out using numerous sources simultaneously.

“dual control”, means a security procedure involving two distinct individuals operating in concert.

“encryption” is the process of encoding information under different levels/standards/protocols of encryption.

“endpoint” refers to a remote computing device that communicates with a network to which it is connected.

“financial institution” for the purpose of this Guideline, refers to:

(a) any bank, non-bank deposit taking institution, cash dealer or payment service provider licensed by the Bank; or
(b) any operator of a payment system, clearing system or settlement system, authorised by the Bank.

“grey box testing" refers to a testing approach in which the tester has a limited knowledge of the environment and its credentials.

“identity and access management” encapsulates people, processes and technology to identify and manage the data used in an IT system to authenticate users and to grant or deny access rights to data and their resources.

“information asset” refers to any piece of data, device or other component of the environment that supports information-related activities. In the context of this guideline, information assets include data, hardware and software. Information assets are not limited to those that are owned by the financial institution. They also include those that are rented or leased, and those that are used by service providers to deliver their services.

"Information Security and Management System" refers to a documented management system that consists of a set of security controls that protect the confidentiality, availability, and integrity of assets from threats and vulnerabilities.

"information system" refers to the set of applications, services, information assets or other information-handling components which includes the operating environment and networks.

"interference", in relation to an information system, means –

a) any impairment to the confidentiality, integrity or availability of computer data;
b) corrupting a computer system by any means; and
c) impairing, by any means, the connectivity, infrastructure or support of a computer system.

"log" refers to the automatically produced and time-stamped documentation of events relevant to a particular system.

"malware" refers to a software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to financial institutions or their information systems.

"multi-factor authentication" refers to the use of two or more of the following factors to verify a user's identity:

(a) knowledge factor, "something an individual knows";
(b) possession factor, "something an individual has"; and
(c) biometric factor, "something that is a biological and behavioural characteristic of an individual".

"network infrastructure" comprises hardware and software, systems and devices which enable computing and communication between users, services, applications and processes.

"recovery point objective" refers to the point to which information used by an activity is to be restored to enable the activity to operate on resumption.

"recovery time objective" refers to the period of time following an incident within which a product or service or an activity is to be resumed or resources are to be recovered.

"red team testing" refers to a controlled attempt based on targeted threat intelligence which focuses on a financial institution's staff, processes and technology with minimal foreknowledge and impact on operations, to compromise the cyber resilience of a financial institution by simulating the tactics, techniques and procedures of real-life threat actors.

"response function" refers to the development and implementation of the appropriate activities to act on a detected cyber event.

"restoration" is the process of copying backup data from secondary storage and restoring it to its primary location or a new location. A restore is performed to return data that has been lost, stolen or damaged to its original condition or to move data to a new location.

"scenario-based testing" refers to a test that assesses a financial institution's response, resumption and recovery plans in order to strengthen cyber resilience. Scenario-based tests address an appropriately broad scope of scenarios, including simulation of extreme but plausible cyber-attacks and are designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans. Scenario-based tests may use cyber threat intelligence and cyber threat modelling to the extent possible to imitate the unique characteristics of cyber threats.

"security zone" refers to a logical segmented section of a network that contains computer or computer systems which have been grouped in accordance with specific security requirements set.

"service accounts" can be privileged local or domain accounts that are used by an application or service to interact with the operating system. In some cases, these service accounts have domain administrative privileges depending on the requirements of the application they are being used for.

"situational awareness" means 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.

"third-party service provider" refers to an entity that is undertaking an activity on behalf of the financial institution or providing a service to the financial institution and includes a member of the corporate group to which the financial institution belongs or an entity that is external to the corporate group, whether located in Mauritius or elsewhere.

"threat intelligence" means, threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes.

"validation" refers to the process of checking the accuracy and quality of source data before using, importing or otherwise processing data.

"vulnerability" refers to a weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats.

"vulnerability assessment" refers to the 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.

PART I - GOVERNANCE

Board and senior management oversight

1. The board and senior management must promote a strong culture of awareness of cyber and technology risk management throughout the institution.

2. Both the board and senior management must collectively possess adequate expertise and experience on matters relating to the cyber and technology risk management and must ensure that their capacity in this regard are regularly updated.

3. The board shall comprise at least one independent or non-executive director with relevant experience in cyber/technology related matters. The board of local banks categorised as Domestic Systemically Important Banks (D-SIBs) shall comprise at least two independent/non-executive directors with relevant experience in cyber/technology related matters. Branches of foreign banks having a local advisory board/committee should ensure that the aforesaid board/committee include at least one member with relevant experience in cyber/technology related matters.

4. The board and senior management must ensure that a comprehensive technology strategy together with the relevant cyber and technology risk management strategy and framework are established and maintained. The strategies shall be aligned with the business strategy of the financial institution.

5. The board is responsible for:

   (i) reviewing and approving at least annually or more frequently depending on the threat landscape, the technology strategy, the relevant cyber and technology risk management strategy and framework and related policies;

   (ii) providing relevant guidance in the development of and approving a cyber and technology risk appetite and tolerance statement that describes the nature and level of cyber and technology risk the institution is willing to assume in order to achieve business goals and the technology strategy;

   (iii) ensuring that it receives regular and timely reports on material cyber and technology incidents, on the evolution of the threat landscape including current and emerging risks, on the findings of internal audits, external audits and testing exercises and on the overall status and effectiveness of the cyber and technology risk management framework;

   (iv) ensuring that cyber and technology risk management matters are adequately discussed at board and other relevant sub-committee meetings;

(v) ensuring that the financial institution, with the approval of the board, appoints a senior officer as a Chief Information Security Officer (CISO);

(vi) ensuring appropriate oversight and coverage of the cyber and technology risks by the control functions and external auditors taking into consideration, inter alia, the requirements of this guideline; and

(vii) promoting a strong culture to cyber and technology resilience.

6. The board of local banks categorised as a D-SIB shall set up a distinct cyber and technology risk sub-committee comprising at least two directors with relevant experience in cyber/technology related matters. The mandate of the sub-committee shall inter-alia include the oversight of the technology strategy, the cyber and technology risk management strategy and the framework and the implementation of cyber/technology-related critical projects. The sub-committee shall receive regular reports on cyber/technology related matters from relevant stakeholders and report on a quarterly basis to the Board. It shall also ensure that the board is promptly apprised of material developments.

7. The board of financial institutions other than local banks categorised as a D-SIB may, at its discretion, delegate the above roles and responsibilities to the Risk Management Committee or to an appropriate sub-committee of the board. In such instances, the Risk Management Committee or the relevant sub-committee of the board shall submit quarterly reports to the board and ensure that the board is promptly apprised on material developments.

8. Senior management is responsible for:

(i) the effective implementation of the technology strategy and of the cyber and technology risk management framework and strategy;

(ii) ensuring that the level of cyber and technology risk assumed by the financial institution is within the risk appetite and risk tolerance defined by the board;

(iii) defining the roles and responsibilities of cyber and technology risk management staff;

(iv) developing key performance metrics and indicators to monitor the cyber and technology risks and the effectiveness of the risk management framework;

(v) developing and reviewing, at least annually or more frequently depending on the threat landscape, the technology strategy, the cyber and technology risk management framework and the relevant policies and processes to manage cyber and technology risks in accordance with the risk appetite of the financial institution;

(vi) ensuring information on the financial institution’s cybersecurity threats and developments are effectively analysed and used for decision making in a timely manner;

(vii) closely monitoring the threat landscape, current trends and potential market developments that may present challenges to cyber and technology risk management so that they can make appropriate and timely changes to the strategy and risk management framework of the financial institution as needed;

(viii) assessing the adequacy and effectiveness of the cyber and technology risk management framework of the financial institution at least annually or upon major changes in the threat landscape, risk profile or in the information system of the financial institution;

(ix) establishing and maintaining a robust cyber and technology risk awareness and training programme for staff and board members;

(x) assessing and validating the effectiveness of the training and awareness programmes;

(xi) promptly escalating material concerns to the board and the relevant sub-committees;

(xii) ensuring that staff members, parties having access to sensitive or critical information, systems, services, infrastructures and other assets and those involved in cyber and technology risk management have an adequate level of skills, experience and expertise and receive relevant trainings on the matter; and

(xiii) ensuring that information on cyber and technology risk events (attempted, suspicious and successful), vulnerabilities and threat intelligence trends are regularly collected and analysed.

The roles and responsibilities of the CISO

9. The CISO shall:

(i) be a senior officer;

(ii) be in the second line of defence;

(iii) be independent of IT operations;

(iv) have an adequate set of skill, expertise and experience in cyber/ technology risk management;

(v) have sufficient resources, including an adequate number of competent personnel; and

(vi) have direct access to the board and to the designated sub-committee of the board.

10. The CISO shall be responsible for:

(i) the development and implementation of the cyber and technology risk management framework;

(ii) providing quarterly reports to the board or to the designated sub-committees of the board on the cyber and technology risk position of the financial institution, including trends in key performance metrics, results of assessment of training and awareness programs, key developments in the threat landscape and key findings from testing exercises, audits and other reviews (as applicable to the relevant governance structures);

(iii) keeping the Chief Risk Officer well informed of cyber/technology risk-related issues, so that the latter can address risks at an Enterprise-Wide level;

(iv) providing support to the board, relevant board sub-committees and senior management on matters related to cyber and technology risk management;

(v) cyber and technology risk management, including producing relevant policies and procedure manuals;

(vi) monitoring compliance to the cyber and technology risk policies and procedures by the financial institution and relevant third-party service providers;

(vii) ensuring adequate cyber and technology oversight of third-party service providers;

(viii) monitoring services provided by third-party service providers in relation to cyber and technology risk management;

(ix) designing and updating the contingency plan with regard to cyber and technology issues;

(x) the implementation of cyber resilience measures;

(xi) ensuring that there is an adequate process in place to report and address cyber-related queries from internal and external parties;

(xii) the investigation of cyber incidents;

(xiii) ongoing monitoring of the evolution of the threat landscape including current and emerging risks; and

(xiv) developing relevant cyber and technology security awareness and training programmes. This includes the evaluation of staff on cyber resilience awareness and participation in the assessment of training needs.

11. Branches and subsidiaries of foreign banks may entrust the roles and responsibilities of the CISO to an appropriate senior officer in the second line of defence and independent of IT operations. The designated senior officer shall report to the group or regional CISO and may rely on the resources of the group/regional office. The board shall ensure that the arrangements in place address all the requirements of the guideline and that there is adequate oversight by the designated officer, the senior management and the board.

Technology strategy

12. Financial institutions shall have a board-approved technology strategy which takes into consideration the objectives of the entire organization and input from all departments and includes:

(i) their vision, including where they are currently and where they aspire to reach over the short term (up to three years) and long term with respect to technology;

(ii) their technology road map detailing the goals and objectives and the steps to be taken to achieve their vision over short term and long-term horizon;

(iii) timelines for critical projects; and

(iv) the associated costs and budgets.

Cyber and technology risk management strategy and framework

13. Financial institutions shall have a board-approved cyber and technology risk management strategy, framework and related policies.

14. Financial institutions can opt to have a standalone strategy, framework and relevant policies for cyber and technology risk management framework or include same in their Enterprise-Wide Risk Management Framework.

15. Financial institutions shall refer to industry best practices including relevant industry standards when designing their frameworks and implement the most effective solutions taking into consideration, inter alia, the complexity of their operations and services, the underlying technology and inherent risks.

16. The cyber and technology risk management framework of a financial institution should:

(i) take into consideration the business strategy and technology strategy as approved by the board and the requirements of the guideline;

(ii) be consistent with the cyber and technology risk appetite and tolerance statement approved by the board;

(iii) document the processes behind the determination of the cyber and technology risk management objectives and risk tolerance;

(iv) document the policies, procedures and controls taking into consideration the requirements of this guideline;

(v) be consistent with the overall risk management framework of the financial institution;

(vi) take into consideration the current and evolving threat landscape, the complexity of the operations, services and technology and risks posed by vendors, other market participants and service providers;

(vii) clearly specify the roles and the responsibilities including accountability for decision-making in respect of identifying, mitigating and managing cyber and technology risks;

(viii) consider the interconnections of the institution with third parties from a cyber and technology risk point of view; and

(ix) be communicated to relevant staff of the financial institution.

17. The cyber and technology risk management strategy and framework, including relevant policies and procedures, shall be reviewed and updated annually, or upon major changes in the threat landscape or in the information system, to reflect the current and evolving threat landscape, threat intelligence and the introduction of new services, technologies and service providers.

18. Branches and subsidiaries of foreign banks may adopt the cyber and technology strategy and risk management framework, including relevant policies of their parent bank provided that they are in line with the requirements of this Guideline and their technology and business strategies.

Control functions

19. The compliance, risk and internal audit (including IT audit) functions shall have the necessary expertise and resources to provide independent and objective assurance on the cyber and technology risk management framework.

PART II – IDENTIFICATION OF CYBER AND TECHNOLOGY RISKS

20. A financial institution shall:

(i) implement an appropriate framework for the identification of cyber and technology risks;

(ii) ensure that all functions, roles, processes, assets (including those involving third-party service providers) and any other data, device(s), component(s) or connection point(s) of the network system are duly identified, classified and documented;

(iii) establish a rating methodology for determining the criticality and sensitivity of individual/system accounts, information assets and other information systems;

(iv) maintain an inventory of all individual and system accounts (including privileged and remote access accounts), cyber/technology services, key roles, processes, information assets, third-party service providers and interconnections together with criticality rating;

(v) regularly conduct risk assessments taking into account critical services, roles, processes (including those involving third-party service providers), information assets and connection points;

(vi) conduct risk assessments when new products, services, technologies, projects or connection points are being implemented and when new information affecting the cyber and technology risks, including the threat landscape of the financial institution are identified;

(vii) maintain an up-to-date and complete network system (including network resources) maps. The map should, inter alia, contain all servers, routers, wireless networks and security devices forming the network system, interconnections as well as all external connection points, dependencies, and data flows with its connected information assets (including those with third-party service providers);

(viii) identify the cyber and technology risks that the institution bears from or poses to its interconnections and coordinate with relevant interconnected entities to, inter alia, work together to address such risks, with the objective of improving the overall resilience of all parties;

(ix) comprehensively document all individual and system accounts, including privileged and remote access accounts, so that it can track all access rights to its information assets; and

(x) review and update all of the above regularly and as and when changes occur in a timely manner such that the risk assessments remain accurate and up to date.

21. A financial institution shall, with respect to exchange of information with customers and third parties:

(i) perform a risk assessment to ensure confidentiality, integrity and availability requirements of data being exchanged are maintained while allowing customers and third parties to connect to its IT systems via APIs; and

(ii) ensure implementation of security features commensurate with sensitivity and business criticality of the data being exchanged.

22. A financial institution is encouraged to:

(i) implement automated tools (such as a centralised asset inventory management tool) to support the classification of critical services, roles, processes (including those involving third-party service providers), information assets and connection points;

(ii) implement automated tools (such as a centralised identity and access management tool) to support the identification and classification of roles, user profiles and individual and system credentials; and

(iii) make use of automated feeds in order to identify emerging risks and update its cyber and technology risk assessment framework.

PART III - PROTECTION

Control implementation and design

23. A financial institution shall:

(i) put in place a robust and effective set of security controls that will enable it to fulfil its security objectives, which should include ensuring:

a. the continuity and availability of its information systems; and

b. the confidentiality, integrity and availability of information stored in its information systems;

(ii) develop its security controls to address all aspects of security, including logical, physical, people and third-party security. The controls should be commensurate to the cyber and technology risks faced by the financial institution and should be consistent with its business goals and risk appetite;

(iii) regularly assess its security controls to ensure that they remain effective and have been applied to all assets, where appropriate, and remain relevant to the evolving cyber and technology risks and threat landscape;

(iv) consider relevant international standards and best practices when developing its security controls;

(v) ensure that cyber and technology resilience are considered at the earliest possible stage in systems planning, implementation and purchasing, as well as during the technology development stage in order to limit vulnerability to the applications and hardware and ensure that security checks are integrated into their structures and procedures from the very beginning; and

(vi) regularly review its information security management system through relevant certification, audits, testing exercises or other appropriate means of assurance. The frequency of the review shall be commensurate with the criticality of the financial institution's assets and services.

Network and infrastructure management

24. A financial institution shall:

(i) set up a secure boundary to protect its network infrastructure through the use of technologies such as, inter alia, a router, firewall or virtual private network. The boundary should distinguish trusted and untrusted areas based on risk profile and criticality of information assets stored within each zone. Reasonable access criteria should be applied within and between each security zone using the concept of least privilege;

(ii) implement network segmentation in accordance with the sensitivity of the systems;

(iii) define baseline systems and security requirements for information systems and system components including devices used for remotely accessing the financial institution network in order to facilitate configuration and security reinforcement of such systems and components;

(iv) use secured network protocols (shell protocols and transport layer security protocols or equivalent) to ensure confidentiality and integrity of information shared on and through the network including remote connections;

(v) establish end-to-end encrypted connection between its branches, customer devices and the system of the financial institution for electronic delivery channels;

(vi) provide for reliability, redundancy and non-repudiation for online financial systems;

(vii) ensure that there are procedures to limit, lock and terminate system and remote sessions after a predefined period of inactivity and when predefined conditions (including unsuccessful attempts) are met;

(viii) incorporate a defence-in-depth security architecture and maintain network and data flow diagrams that describe hardware, applications, network elements, internal and external communications and the type of information shared. The full network and data flow diagrams should be kept up to date;

(ix) implement technical measures to prevent the execution of unauthorised code on institution-owned or managed devices, network infrastructure and system components;

(x) ensure that changes to system configurations are strictly controlled and monitored and that programmes that can alter or override system configuration are restricted. This should also be applicable to remote connections;

(xi) implement technologies and solutions to detect and block actual and attempted attacks or intrusions. This may include intrusion detection or prevention systems, endpoint security solutions (e.g. antivirus, a firewall, or a host intrusion detection system (HIDS) or host intrusion prevention system (HIPS)) or any other relevant solutions (e.g. an access gateway or a jump box), including on devices and in environments used for remote connections;

(xii) ensure that non-controlled devices are prevented from connecting to the internal network from inside and outside;

(xiii) ensure that it has in place policies and procedures on activities on the internal network that should be logged and monitored for inappropriate use or attempts to access business systems based on their internal risk assessment;

(xiv) ensure that the network infrastructure is scanned regularly to detect rogue devices and access points;

(xv) ensure that users are prevented from installing unauthorised applications; and

(xvi) segment its network infrastructure with adequate security policies commensurate to the risks it faces and which define proper access policy to systems and applications. Sensitive traffic between systems and zones should be segregated using network management.

Logical security management

25. A financial institution shall:

(i) identify and restrict logical access to its system resources to the minimum required for legitimate and approved work activities, according to the principle of need to know and least privilege;

(ii) establish policies, protocols, and controls for access privileges and how they should be managed. The access privileges should be promptly revoked or adjusted upon change in employment status of employees and should be reviewed at least annually;

(iii) establish strong security standards to deploy Application Programming Interfaces (APIs) which should as a minimum include:

a. measures to protect API keys of access tokens by implementing a comprehensive key management lifecycle that incorporates key generation, usage, storage, rotation, and eventual retirement;

b. strong encryption standards for transmission of data through APIs;

c. documenting access of third parties through APIs, including details such as identity of the third party, the data being accessed and the timing of the access; and

d. establishment of measures to revoke API keys or access tokens in case suspicious activities are detected;

(iv) establish dual control for access to critical systems, services, infrastructures and other assets;

(v) regularly review access to the information system to detect any unnecessary access or rights;

(vi) ensure that unauthorised access to systems is blocked;

(vii) ensure that there is limited and controlled access (logical, and/or remote access) to critical systems, services, infrastructures and other assets and that same are duly monitored logged with relevant audit trail;

(viii) restrict system administration privileges solely to operational requirements;

(ix) regularly review all access privileges according to defined procedures;

(x) establish procedures for allocating privileged access which should also include delegated access on an on-demand or event-by-event basis for specific administrative activities as defined by the bank. The use of service accounts for administrative purposes should be tightly regulated and monitored. User and administrator accounts should be nominative and identifiable;

(xi) ensure that appropriate logs are maintained to identify access and activities by privileged users and users having access to critical systems, services, infrastructures and other assets or functions and any other systems, functions or applications as determined by the financial institution based on its risk assessments;

(xii) all privileged access or access to critical systems, services, infrastructures and other assets, functions or applications shall be monitored to detect anomalous behaviour;

(xiii) establish a policy that covers all aspects of its authentication processes which is compliant with industry requirements;

(xiv) implement controls to prevent unauthorised privilege escalation;

(xv) develop capabilities, such as people, processes, and technology, to track privileged users' actions and access to sensitive systems in order to detect and prevent anomalous behaviour and alert necessary personnel;

(xvi) implement controls commensurate to the criticality of the data to protect and encrypt data at rest and in transit and to ensure that processing of data is done in a secured environment;

(xvii) ensure that access rights of all departing employees are promptly revoked. The departing employees should be required to return all information assets that belong to the financial institution, including important documentation, equipment, software and authentication hardware;

(xviii) ensure that access rights of employees are promptly adjusted upon change in employment status;

(xix) establish a password policy which would enforce strong password controls for users' access to systems, which would include inter alia:

a. use of one-time password for first logon and requiring change of password thereon;

b. a minimum password length requirement;

c. an alphanumeric password requirement;

d. establishing adequacy criteria for passwords based on the history of password used and commonly used passwords; and

e. changing of passwords on a regular basis;

(xx) establish credential requirements which among others take into consideration the risk level (e.g. multi-factor authentication for higher risk access);

(xxi) ensure that multi-factor authentication for employees and authorised third-parties is implemented for the following:

a. all administrative accounts for critical operating systems, databases, applications, security appliances or network devices;

b. all accounts for critical systems, services, infrastructures and other assets/applications which directly allow access to customer information through the internet (e.g. web-based applications, etc); and

c. all instances of remote access which allows users connect to the network system of the financial institution; and

(xxii) ensure that the processing of special categories of data, such as the use of biometric data for authentication purposes, is in line with the requirements of the Data Protection Act 2017.

26. A financial institution shall establish an appropriate framework in respect of multi-factor authentication for electronic delivery channels. This shall amongst others take into consideration the nature and the level of risk involved in the transaction, the value of transaction and the recurrence of the transaction. Higher risk transactions shall be subject to multi-factor authentication.

27. A financial institution is encouraged to:

(i) automate the administration of information system access accounts to, inter alia, disable and/or delete disabled, temporary and emergency accounts after a predetermined period of time and to detect unauthorised access;

(ii) implement automated identity and access management tools to ensure that all systems promptly update each other and for recertification of access rights;

(iii) implement tools for automatic notifications to staff in charge of granting or revoking access to the information system upon change of employment status; and

(iv) make use of one-time password for critical applications.

Encryption and other cryptographic materials

28. Financial institutions shall:

(i) establish requirements with regard to data encryption and use encryption and general cryptographic controls in accordance with recognised standards and processes, which address issues such as algorithm, key length, and key generation, among others. The encryption level should take into consideration the criticality of the underlying data/ information assets. The encryption keys shall be stored separately from virtual images and the data;

(ii) implement controls to prevent unauthorised access to encryption keys, hard/soft tokens and other cryptographic materials. Separate policies and procedures should be specified for the management and access to these cryptographic materials. The financial institution may hold the cryptographic materials and manage cryptography through the use of hardware security modules, virtual cryptography tools, cloud-based security tools or a combination of these or retain the services of a reputed third-party service provider for the management of the cryptographic materials. Where the financial institution opts for the key management services and other cryptography related services of a third-party service provider, it shall ensure that:

a. there are appropriate arrangements in place by the third-party service provider to secure them;

b. it understands and is satisfied with the circumstances in which the third-party service provider may use or access the keys, hard/soft tokens and other cryptographic materials; and

c. there is appropriate segregation within the service provider between access to keys and, where applicable, access to customer information; and

(iii) control access to cryptographic keys for core banking services. The financial institution may grant a third-party service provider access to the cryptographic keys to deliver pre-agreed critical/security services.

Physical security management

29. A financial institution shall:

(i) implement appropriate measures to protect its premises, sensitive areas and data centres from unauthorised access and from natural and other hazards;

(ii) identify and restrict physical access to information systems to the minimum required for legitimate and approved work activities, according to the principle of need to know and least privilege;

(iii) ensure that appropriate logs are maintained to identify physical access to information systems;

(iv) ensure that there is limited physical access to critical systems, services, infrastructures and other assets and that same are duly logged. Critical systems, services, infrastructures and other assets should also have additional physical controls such as being monitored by CCTV cameras and being secured by an alarm. The monitoring and management of CCTV cameras should be outside the control of the IT department;

(v) ensure that access rights are promptly cancelled or adjusted upon change in employment status of employees; and

(vi) maintain an inventory of their technology assets including their criticality rating, physical location (for instance, servers and their respective locations).

Change and patch management

30. A financial institution shall:

(i) have policies, procedures and controls in place for change management, including criteria for prioritising and classifying the changes;

(ii) ensure that all related information is backed up and a roll-back strategy is created before implementing changes to information assets to ensure that they are evaluated, checked, reviewed and accepted;

(iii) establish a patch management process to ensure that relevant functional and non-functional patches (e.g. corrections for security vulnerabilities and program bugs) are enforced within a period commensurate with the patches' criticality and the financial institution's information systems;

(iv) ensure that patches and changes are thoroughly tested before deployment;

(v) specify the processes for reviewing, authorising, and enforcing emergency modifications; and

(vi) have in place appropriate recovery plans.

31. A financial institution is encouraged to consider using standardised configuration of IT resources to facilitate its patch management process.

Technology refresh management

32. A financial institution shall:

(i) avoid using outdated and unsupported hardware or software, including legacy technologies;

(ii) develop a technology refresh plan for replacing outdated and unsupported hardware or software, including legacy technologies, that are reaching end of support (EOS);

(iii) ensure that a risk evaluation for outdated and unsupported hardware and software, including legacy technologies, is duly undertaken to determine the risk of continuing to use them and the appropriate risk reduction mechanisms for maintaining the risk at an acceptable level. The risk evaluation and risk reduction plan should be duly approved by the board or the designated sub-committee of the board and senior management; and

(iv) ensure that outdated and unsupported hardware or software, including legacy technologies are regularly scanned to identify potential vulnerabilities.

People management

33. A financial institution shall ensure that:

(i) all staff, including contractors and service providers, are competent and skilled enough to conduct the assigned roles and handle technology risks;

(ii) appropriate background checks and fit and proper tests are conducted on staff, including contractors and service providers and their staff, commensurate with the criticality of the data and information systems to which they would have access; and

(iii) physical and logical behaviour patterns (e.g. network use patterns and work hours, etc.) are monitored for critical information assets/systems to identify anomalous activities.

34. A financial institution is encouraged to implement innovative solutions (e.g. data analytics, machine learning and artificial intelligence, etc.) to detect and respond to threat activity in real time.

Third-party service providers

35. Financial institutions shall conduct due diligence on third-party service providers before using their services. The due diligence shall be duly documented and approved.

36. The extent of due diligence to be performed, including the requirements for onsite audits or remote audits, shall be commensurate with materiality of the services and of the IT assets involved and the level of reliance the financial institution places on the third-party service provider to maintain effective security controls.

37. The due diligence on a third-party service provider in respect of material services shall, inter alia, include:

    (i) the adequacy of the third-party service provider's risk management and internal control systems, information security capabilities and security controls including the controls for protecting the confidentiality, integrity and availability of data taking into consideration the findings of vulnerabilities assessment, penetration testing, audit and/or other reviews provided by the third-party service provider, where relevant;

    (ii) the third-party service provider's compliance with the requirements of this Guideline, the applicable data protection, confidentiality and information security regulations or other legislations and adherence to international IT standards;

    (iii) the willingness and ability of the third-party service provider to service commitments even under adverse conditions, for instance, in the event of a cyber-attack or data theft;

    (iv) the ability of the third-party service providers to recover outsourced systems and IT services within the stipulated recovery time objective and recovery point objective;

    (v) the verification of whether the personnel of the third-party service provider (including employees and subcontractors) with access to customer information are subject to adequate background screening, security training, access approvals and confidentiality arrangements;

    (vi) forward looking assessment of the financial and operational resilience of the third-party service provider; and

    (vii) an assessment of the proven track record of at least three years of the third-party service provider for such services.

38. With respect to third-party service providers having access to its information assets or hosting its information assets, a financial institution shall:

(i) ensure that the third-party service provider is complying with all requirements of the guideline;

(ii) ensure that the necessary due diligence is carried out before onboarding the third-party service provider;

(iii) be aware of the information security measures and controls established and ensure that they are in line with the requirements of the guideline;

(iv) maintain an updated inventory of third-party service providers which have access to its information assets together with their criticality rating;

(v) ensure that the contracts with third-party service providers are duly executed, do not consist of any clause that would hinder the Bank from exercising its supervisory powers, and include relevant provisions:

a. to ensure the continued effectiveness of its cyber and technology risk management framework;

b. to ensure compliance with relevant laws in Mauritius (e.g. The Cybersecurity and Cybercrime Act 2021, Data Protection Act 2017, ICTA, etc.) or to relevant and equivalent laws at all times;

c. to impose confidentiality obligations on the third-party service provider which are in line with the underlying objective of section 64 of the Banking Act 2004 or section 18 of the National Payment Systems Act 2018, as relevant;

d. to ensure compliance with the record keeping obligations as set out in the Banking Act 2004;

e. to create the obligation of the third-party service provider to provide reasonable notice in the event of changes in subcontractor or change in location where the data in its possession is stored or processed;

f. on the right of audit (including remote audit) by the Bank, the financial institution, its external auditor, or any third-party service provider appointed by the Bank, the financial institution or its external auditor. The cost of audit by any third-party service provider appointed by the Bank shall be borne by the financial institution;

g. on the right of access by the Bank, the financial institution or its external auditor to relevant audit reports/reports of other tests conducted by or arranged by the third-party service providers;

h. on the right of the Bank or any third-party service provider appointed by the Bank to promptly take possession of all services and data relating to the financial institution in the event the Bank decides to revoke the licence of the financial institution or appoints a conservator. The procedures for executing the change of ownership request and for ensuring continuity of services during this process should be duly documented and agreed with the third-party service provider;

i. on the right of the financial institution to terminate the agreement where, inter alia, the financial institution has concerns on the third-party service provider, the location of the data and the subcontractors involved;

j. to ensure the obligation of the third-party service provider, where applicable, to cooperate with the Bank and provide access to information required by the Bank, the financial institution, its external auditor, or any third-party service provider appointed by the Bank;

k. on exit strategies which are comprehensive and well documented. The exit strategies shall be regularly reviewed to ensure that they remain adequate and effective. The exit plan shall, as a minimum, include the following:

    1. agreed process and procedures including reasonable timeframe for deletion of all data (bank and customer data) of the financial institution;

    2. assurance from the third-party service provider through relevant independent reports/certificates that all data of the financial institution (including any backup) is rendered permanently irrecoverable and inaccessible in a timely manner after termination of the contract;

    3. transferability of services (to a third party or back to the financial institution) for the purpose of continuity of service; and

    4. identification of alternative solutions to allow for business continuity throughout and after the transition phase;

l. incident management process, including the roles and responsibilities of each party;

m. the governing law; and

n. dispute resolution considering the chosen governing law for the contract;

(vi) conduct third-party risk assessment at the outset and on a periodic basis which shall, inter alia, include:

a. assessing the adequacy of the cyber and technology resilience capabilities of the third-party service provider;

b. identifying the associated risks (including cyber/IT related risk and concentration risk by the third-party service provider and by geographical location), the vulnerabilities, the benefits and the sustainability of the services and the impact on the risk profile of the financial institution;

c. evaluating of criticality and sensitivity of the IT assets and the materiality of the services;

d. evaluating the impact of changes required to processes and procedures;

e. evaluating the adequacy of the internal cyber/technology risk management framework including availability and adequacy of the skilled and experienced in-house resources for an effective deployment and oversight of the services;

f. an assessment to ensure that data, including customer information, are logically segregated and encrypted;

g. identifying the roles and accountabilities of the financial institution and the third-party service provider;

h. assessing the adequacy of the control framework;

i. the impact of possible risk events including failure of the third-party service provider, disruption of services, exit and the implications for transferring services in-house or to another third-party service provider, if required;

j. the adequacy of contingency and exit plan including the interoperability and portability of data and services;

k. the risk of foreign authorities having access to its data;

l. the relevant legal and regulatory requirements;

m. ensuring the compliance of the third-party service provider with the requirements of this guideline; and

n. assessing the track record of the third-party service provider;

(vii) ensure that there are appropriate procedures in place to isolate or block its third-party connections if there is a cyber or technology incident and/or a risk of contagion;

(viii) be aware of the cybersecurity/information security measures established by third-party service providers having access to customer information and other critical information assets and ensure that such security measures are equivalent, if not more stringent, than the controls which are implemented on premise for similar information assets;

(ix) ensure that it is satisfied with the cyber and technology resilience capabilities of third-party service providers having access to customer information and other critical information assets, by periodically using tools such as certification, external audits, testing exercises such as vulnerability assessment, service level agreements and key performance indicators in this respect;

(x) implement appropriate security controls that detect and prevent intrusions from third-party connections; and

(xi) comply with the Guidelines on Outsourcing by Financial Institutions and the Guideline on Use of Cloud Services, as applicable.

39. Financial institutions shall ensure that third-party service providers involve in the conduct of independent audits, vulnerability assessments, penetration testing and other testing exercises are duly accredited by a reputed body.

40. A financial institution is encouraged to automate the process for detection and prevention of unauthorised access from third-party service providers.

Rotation and cooling off periods for third-party service providers

41. No third-party service provider shall be responsible for the conduct of external independent assessments, penetration testing and vulnerability assessments for a continuous period of more than 3 years.

42. Where a third-party service provider has been responsible for the conduct of external independent assessments, penetration testing and vulnerability assessments for a continuous period of 3 years or less, that firm shall not be entrusted the responsibility of the aforementioned tasks before a period of 2 years from its last assignment.

Hosting of customer information, information assets and information systems outside Mauritius

43. Financial institutions shall conduct relevant due diligence on the countries involved.

44. Financial institutions shall be aware of the location (city and country) where their customer and other material information assets/systems will be hosted and shall ensure that:

(i) they consider the risk of foreign authorities having access to their data and require the service provider to advise of instances where it was legally bound to disclose clients' data to foreign authorities in the past and of any such potential disclosures in the future (if available) in their risk assessment;

(ii) the governing law and jurisdiction chosen are suitable for enforceability of the contractual provisions in case of breach thereof on part of the service provider;

(iii) data protection laws in the foreign jurisdiction where the data is hosted and processed are in line with the Mauritian data protection laws or data protection laws which are equivalent to the Mauritian data protection laws;

(iv) the foreign jurisdiction's laws or regulations do not place any restrictions regarding:

a. on-site examination audit and access rights of the Bank, the financial institution, its external auditors or any third party appointed by them; and

b. access to the information by the Bank, the financial institution, its external auditors or any third party appointed by them;

(v) there are appropriate contractual provisions allowing the financial institution to terminate the agreement in case there is a change in the location where they have concerns with the new location;

(vi) the foreign authorities do not have access to the data of the financial institution. Where the service provider is required to disclose data of the financial institution to an authority of the countries where the data is located, following an order issued by a court or regulatory authority of competent jurisdiction, the agreement entered with the service providers should contain the following obligations to cater for such instances:

a. the service provider shall use reasonable efforts to notify the financial institution before any such disclosure is made so that the financial institution may seek by legal means to prevent or limit such disclosure, except to the extent that providing such prior notice to the financial institution is prohibited by law or regulatory authority; and

b. where the service provider is unable to give such prior notice due to legal or regulatory constraints, it should implement appropriate legal and protective measures in the interest of the financial institution; and

(vii) the Bank is duly informed by the financial institution of any disclosure made by the service provider in the event the latter is required to disclose data of the financial institution to an authority of the countries where the data is located, following an order issued by a court or regulatory authority of competent jurisdiction.

45. Financial institutions shall ensure that the due diligence under sections 43 and 44 are conducted by a competent officer of the financial institution or a reputed firm, as deemed appropriate.

46. Financial institutions shall establish a pre-agreed list of locations where its data will be processed with the service provider. Where data is processed in a location outside the pre-agreed list, the financial institution shall ensure that:

(i) such instances are limited to cases involving processing of individual transactions initiated by end users of the financial institution;

(ii) it is promptly informed by the outsourced service provider of the location (city and country) where its data has been processed including the rationale thereof; and

(iii) it obtains assurance from the service provider that the processing of data was done in a secured environment and that its data has been permanently removed from that location and transferred to a pre-agreed location within a reasonable timeframe.

Secure coding in application development

47. Financial institutions shall implement secure coding, source code review and application security testing. For critical applications, financial institutions shall abide with relevant international standards.

48. The standard of secure coding and source code review should encompass such areas as secure programming techniques, input validation, output encoding, access control, authentication, encryption, errors and exceptions.

49. A policy and procedure for using open-source software code and third-party software should be developed. The policy shall, inter alia, require that these codes are reviewed and tested before integration into the software/system of the financial institution.

50. The financial institution shall ensure that its software developers are qualified or have the requisite knowledge and abilities to implement secure coding and application security standards while developing applications.

End-user computing

51. Financial institutions shall implement an appropriate risk management framework before deploying applications developed by end users and which are not maintained by its IT department. This shall, among others, include adequate testing and approval.

PART IV - DETECTION

52. A financial institution shall:

(i) monitor internal and external variables by using a combination of signature monitoring for known vulnerabilities and behaviourally based detection mechanisms;

(ii) identify, consider and record the baseline profile of user/device activities based on the risk assessment conducted during the identification process to aid in detecting deviation from the baseline such as anomalous activities and events;

(iii) actively monitor for phishing campaigns targeting the financial institution or its customers;

(iv) with regard to electronic delivery channels:

a. establish a real-time monitoring system to detect suspicious or fraudulent transactions; and

b. establish a system for notification of transactions above a certain limit and of higher risk transactions to their customers, including relevant details of the transaction such as type of transaction, amount of the transaction and timing of the transaction;

(v) monitor user activity, exceptions, cyber and technology risk events, connections, external service providers, devices and software and analyse same for unusual behaviour;

(vi) ensure that the effectiveness and appropriateness of its detection capabilities are regularly reviewed and enhanced and that related staff receive relevant training on the matter;

(vii) identify warning signs for detecting cyber and technology incidents and for determining if breaches have occurred;

(viii) employ a defence-in-depth strategy by implementing multi-layered detection controls that cover individuals, procedures, and technologies, with each layer acting as a safety net for the layers before it; and

(ix) be able to track cyber and technology incidents and quickly change its security controls, working in cooperation with other stakeholders.

53. A financial institution is encouraged to:

(i) set up a Security Operations Centre or equivalent for tracking and detecting anomalous activities and events; and

(ii) design and implement automated systems (e.g. a security information and event management (SIEM) system) and/or relevant processes to capture, centralise, and compare event information from various sources, as well as log analysis, to constantly track the risk environment.

PART V – RESPONSE AND RECOVERY

Business continuity plan

54. A financial institution shall have a board approved business continuity plan which, as a minimum:

(i) identifies its critical services, key roles, processes, information assets and third-party service providers;

(ii) defines its recovery point objectives and recovery time objectives;

(iii) considers extreme but plausible scenarios of cyber and technology incidents or other incidents which would impact its systems;

(iv) includes business impact analyses to assess the potential impact of those scenarios quantitatively and qualitatively;

(v) sets out recovery and response plans, dependent on the various scenarios, to safeguard critical assets, maintain critical services and achieve its recovery objectives;

(vi) ensures that its recovery and response team have the necessary skills, experience and training to address cyber or technology incidents;

(vii) defines parameters regarding detection of cyber or technology incidents which would trigger its recovery and response plans;

(viii) ensures that the response and recovery plans of third-party service providers are satisfactory;

(ix) considers continuity measures to mitigate the impact of failures of third-party service providers. For material services, financial institutions shall ensure that:

a. business continuity requirements such as disaster recovery plans, recovery time, recovery point objectives, maximum allowable loss of data, plans for communicating incidents and the frequency of testing of adequacy and effectiveness of these plans are developed, documented and, where appropriate, agreed with the third-party service provider;

b. the business continuity plans of the third-party service provider are regularly tested. The financial institution should be involved in the testing, as relevant, and should have access to the report on the testing exercises. The business continuity plan of the third-party service provider shall be ideally certified or mapped to internationally recognised standards;

c. appropriate system resiliency and network redundancy in the event of disaster are catered for in the third-party arrangements. Such network redundancy and resilience capabilities shall be tested regularly; and

d. the third-party service provider has adequate plans and resources to ensure the financial institution's continuity of operations, including recovery and resumption capabilities;

(x) includes the setting up of disaster recovery sites which are geographically separated from the primary site, so that both sites will not be impacted by a disruption in a particular location, and which are regularly maintained and tested to ensure they are fit for business continuity;

(xi) ensures there is dual connectivity between their main premises, disaster recovery sites and any alternate data centres (within or outside Mauritius) from two or more distinct Internet Service Providers using different network paths;

(xii) ensures that there are procedures to conduct ex-post investigation of the cause of the cyber or technology incident, implement necessary measures to avoid similar happenings and integrate the findings into its cyber and technology risk management framework; and

(xiii) ensures that its scenarios and business impact analyses and recovery and resolution plans are reviewed on an annual basis to account for changes in the threat landscape and changes in recovery objectives.

Response and recovery plan

55. A financial institution shall have a board approved response and recovery plan for cyber and technology incidents which, as a minimum:

(i) identifies staff and other external stakeholders who are essential to deal with such incidents and who would be alerted in case such an incident is detected;

(ii) sets out the policies, procedures, roles and responsibilities to respond to and recover from cyber and technology incidents;

(iii) focuses on recovery of critical business operations, supporting processes, information assets and their interdependencies to avoid adverse effects on its operations and on the financial system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions;

(iv) sets out the criteria for prompt escalation of cyber or technology incidents to the board or senior management based on the risk posed by the incident;

(v) ensures that, upon detection of an incident, a thorough investigation is conducted to determine the nature of the incident and the extent of the damage caused by the incident;

(vi) sets out the immediate actions to be taken to prevent further damage and to contain a cyber or technology incident;

(vii) ensures that, after the cyber or technology incident is contained, key components of the incident are eliminated through inter alia, identifying all affected systems in the financial institution so that they can be remediated, carrying out malware analysis and checking for any response from the attacker; and

(viii) includes details of internal and external stakeholders, including the Bank, the information that has to be shared and reported together with relevant timeframes, including in case of emergency.

56. The response and recovery plan shall be made available to relevant staff and be readily accessible in the event of an emergency.

Data integrity

57. A financial institution shall:

(i) store backup information at an alternate site, both online and offline, which should be safeguarded by protective and detective controls;

(ii) establish a system and data backup strategy with appropriate frequency of backup which is based on the criticality of the information;

(iii) ensure that the restoration of its system and data backups can be carried out with minimum downtime and limited disruption, in line with recovery objectives;

(iv) test the restoration of its system and data backups to validate the effectiveness of its backup restoration procedures. The frequency shall be commensurate to the criticality of the information and be at least twice a year for critical information and systems; and

(v) ensure that any backup data is protected at rest and in transit to ensure its confidentiality, integrity and availability.

Forensic readiness

58. With a view to facilitating forensic investigation, a financial institution shall:

(i) consider different threat scenarios and determine the types of logs and other pieces of digital evidence that should be collected;

(ii) ensure that the logs and other digital evidence are collected, handled and stored securely and are duly backed up;

(iii) develop an internal policy for the retention of digital evidence and logs. As a minimum, critical logs and digital evidence shall be stored for a minimum of 7 years;

(iv) train its staff such that all those involved in an incident understand their responsibilities related to handling of digital evidence;

(v) ensure that staff specifically designated to conduct forensic investigation have the necessary knowledge and expertise to handle the digital evidence; and

(vi) periodically review its forensic readiness procedures in light of new knowledge and experience.

PART VI – ASSURANCE AND TESTING

59. A financial institution shall test the adequacy of its information security controls through well-documented assurance and testing programmes. The nature and frequency of the reviews and tests must be commensurate with:

(i) the evolution of the threat landscape;

(ii) the criticality and sensitivity of the information asset;

(iii) the consequences of an information security incident;

(iv) the risks associated with exposure to environments where the regulated entity is unable to enforce its information security policies; and

(v) the materiality and frequency of change to information assets.

60. A financial institution shall ensure that the results of reviews, audit and testing exercises are duly reported to the board or designated sub-committees of the board and senior management.

61. A financial institution shall ensure that the assurance (excluding internal audit) and testing programme (including the scope) are reviewed and approved by the board or designated sub-committees of the board at least annually or when there is a material change to information assets or the business environment. The internal audit plan shall be approved by the audit committee of the board at least annually or when there is a material change to information assets or the business environment.

Control functions

62. The compliance function shall ensure adherence to applicable laws, rules and regulations and conduct periodic reviews thereon.

63. The risk and internal audit (including IT audit) functions shall conduct periodic reviews of the cyber and technology governance and risk management framework of the financial institution to, inter alia, ensure that:

(i) the frameworks are:

a. in line with the requirements of this guideline and relevant standards and in compliance with framework approved by the board and senior management;

b. effective and adequately mitigate the cyber and technology risks faced by the financial institution; and

(ii) all policies, procedures and processes are duly being complied with.

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

65. The compliance, risk and internal audit (including IT audit) functions shall ensure that all aspects of the framework are covered over a period of not more than three years.

66. Branches and subsidiaries of foreign banks may rely on reviews conducted by the compliance, risk and internal audit functions of their parent bank. However, they should be able to demonstrate appropriate oversight and control on the scope, frequency, findings and risk mitigating plans of the reviews conducted by their parent bank.

External independent audit

67. Financial institutions should have their governance and cyber and technology risk management frameworks audited, against the requirements of the guideline and relevant industry standards, on a periodic basis, by external independent, competent and reputed assessors. The scope and frequency of the independent assessment should be risk-based and include IT security audit. Critical systems, services, infrastructures and other assets as well as electronic delivery channels shall be covered annually and all areas shall be covered within a two-year cycle for D-SIBs and within a three-year cycle for other financial institutions. The assessors shall report to the board or the designated sub-committee of the board on the effectiveness of the cyber and technology risk management framework as well as on its maturity model (e.g. an assessment of the cyber and technology controls, methods and processes against a clear set of external benchmarks).

68. Branches and subsidiaries of foreign banks may rely on resources available at their parent bank for conducting the external independent audits. However, they should be able to demonstrate the independence and competence of the respective auditors.

69. In cases where the Bank finds it necessary, it may instruct a financial institution to undergo an external independent audit of its governance, systems and processes related to cyber and technology risk management. The cost of the assessment shall be borne by the financial institution.

70. Financial institutions may, in the case of services provided by third-party service providers, including the management of information assets, take into consideration reports of reviews, testing and other audits commissioned by the third-party service providers where they are satisfied with, inter alia,

- the plan and the scope of the audit/assessment and the reports; and

- the independence and competence of the auditors/assessors involved.

71. Financial Institutions shall ensure that they are duly apprised of the results of the exercise commissioned by third-party service providers and are satisfied with the remediation plan.

Testing

72. A financial institution shall ensure that testing is conducted by appropriately skilled and functionally independent specialists (internal to the financial institution or external specialists). Testing include vulnerability assessment, scenario-based testing, penetration testing and red team testing.

Vulnerability Assessment

73. A financial institution shall establish a process to conduct regular vulnerability assessment (VA) on their information systems to identify security vulnerabilities and ensure risk arising from these gaps are addressed in a timely manner. The frequency of VA should be commensurate with the criticality of the information system and the security risk to which it is exposed.

74. As a minimum, the critical systems, services, infrastructures and other assets of a financial institution shall be subject to VA by independent specialists on an annual basis.

75. The scope of the VA should, as 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.

76. A financial institution shall perform VA before any deployment or redeployment of new or existing services supporting major critical services, applications and infrastructure components for fixing bugs and weaknesses, consistently with change and release management processes in place.

77. A financial institution is encouraged to perform vulnerability scanning on an ongoing basis, rotating among environments in order to scan all environments throughout the year.

Scenario-based testing

78. A financial institution shall carry out scenario-based testing exercises at least on an annual basis or upon major changes in the threat landscape to validate its response and recovery, as well as communication plans against cyber threats and technology incidents.

79. Depending on the exercise objectives, a financial institution shall involve relevant stakeholders, including senior management, business functions, corporate communications, crisis

management team, service providers, and technical staff responsible for cyber threat and technology incident detection, response and recovery.

Penetration Testing

80. A financial institution shall carry out penetration testing to obtain an in-depth evaluation of its cyber and technology defences. A combination of black box and grey box testing should be conducted in this regard. The penetration testing should include both the production and test environment.

81. The frequency of penetration testing should be determined based on factors such as system criticality and the system's exposure to cyber and technology risks. For systems that are directly accessible from the internet and for critical infrastructure, assets, systems, penetration testing shall be conducted by independent specialists immediately after deployment or whenever these systems undergo major changes or updates and thereafter on an annual basis.

Red team testing

82. D-SIBs shall perform red team testing to test and validate the effectiveness of their cyber and technology defence and response plan against prevalent cyber threats and technology incidents.

83. Other financial institutions are encouraged to perform red team testing. Where the Bank finds it necessary, it may require a financial institution to conduct red team testing. The cost of the red team testing shall be borne by the financial institution.

84. The objectives, scope and rules of engagement should be defined before the commencement of the exercise and the exercise should be conducted in a controlled manner under close supervision to ensure the activities carried out by the red team do not disrupt the financial institution's production systems.

85. The threat scenario should be designed and based on challenging but plausible cyber and technology incidents as well as real life attacks.

86. The financial institution shall design the exercise scenario by using threat intelligence that is relevant to their threat environment to identify threat actors who are most likely to pose a threat to the financial institution and identify the tactics, techniques and procedures most likely to be used in such attacks.

87. The frequency of the different audits and testing exercises outlined above has been summarised in the table below for ease of reference.

Minimum testing frequency	**Tests**
Ongoing basis	Vulnerability scanning

Minimum testing frequency	**Tests**
Before any deployment/redeployment of new or existing services supporting major critical services, applications and infrastructure components	Vulnerability Assessment
Immediately after deployment of critical systems, services, infrastructures and other assets and systems that are directly accessible from the internet or whenever these systems undergo major changes or updates	Penetration Testing
Major changes in threat landscape	Scenario-based testing
Annual	Vulnerability Assessment of critical systems, services, infrastructures and other assets.
	Scenario-based testing
	Penetration testing for critical systems, services, infrastructures and other assets and for systems that are directly accessible from the internet
	External independent audit of the governance and cyber and technology risk management frameworks, including an IT security audit, **for critical systems, services, infrastructures and other assets as well as electronic delivery channels** against the requirements of this guideline and relevant industry standards
Risk-based approach	External independent audit of the governance and cyber and technology risk management frameworks, including an IT security audit, against the requirements of this guideline and relevant industry standards (2-year cycle for D-SIBS and 3-year cycle for other financial institutions).
	Compliance, risk and internal audit reviews (3-year cycle).
	Red team testing

PART VII - SITUATIONAL AWARENESS

Cyber and technology threat intelligence

88. A financial institution shall:

(i) consider threats to confidentiality, protection, privacy, integrity and availability of its data and damage to its reputation that could result from such threats;

(ii) include, in its threat analysis, threats which could trigger extreme but plausible cyber and technology events, even if they are considered unlikely to occur or have never occurred in the past;

(iii) analyse the information gathered on its cyber and technology threat landscape in conjunction with both internal and external business and system information so as to foresee and prepare against cyber-attacks;

(iv) consider threat information arising from itself, its interconnected counterparties and other financial institutions, both on successful incidents as well as near misses; and

(v) make threat intelligence available to the appropriate staffs having the responsibility to develop the strategic cyber and technology risk management framework of the financial institution and ensure that all cyber and technology risks mitigation measures implemented are threat informed.

Information sharing

89. Financial institutions shall establish a communication policy, including a trusted communication channel for timely information sharing with relevant stakeholders, including the Bank.

90. Financial institutions shall identify the types of information to be shared, as well as the conditions under which the information will be shared, with the relevant stakeholders.

PART VIII - LEARNING AND EVOLVING

91. A financial institution shall:

(i) gather information on vulnerabilities and cyber incidents both within and outside the financial institution, including both successful intrusions and near misses;

(ii) analyse the information gathered to determine the impact on its cyber and technology risk management framework and review same accordingly;

(iii) monitor technological developments and cyber and technology risk management processes which may be used to counter existing and emerging threats and implement same where relevant;

(iv) circulate relevant cyber and technology security materials to its staff whenever necessary, including when prompted by actual cyber and technology events;

(v) implement and regularly monitor indicators to measure the effectiveness of its cyber and technology risk management framework; and

(vi) monitor its progress in developing and enhancing its cyber and technology risk management framework from its current state to a more mature stage. The financial institution may implement a maturity model to document its progress.

92. A financial institution is encouraged to analyse findings from audits, management information, incidents, near misses, tests, exercises and external/internal intelligence to find any correlation which could be used to improve its cyber and technology risk management framework.

93. A financial institution is encouraged to have a proactive approach to its cyber and technology security practices by predicting and anticipating future events, based on analysis of current information and trends.

Security awareness and training

94. A financial institution shall:

(i) develop a robust cyber and technology security awareness and training programme for its staff, senior management and board. The awareness programme should be conducted at least annually. The awareness programme should at a minimum provide guidance on how to detect and respond to cyber and technology incidents and provide an outline of existing and emerging vulnerabilities and cyber threats and technology incidents. The awareness and training programme should also be part of the onboarding programme for new staff;

(ii) ensure that there is an appropriate awareness and training programme for staff involved in the cybersecurity and technology risk management;

(iii) regularly review the awareness and training programme to ensure that it incorporates up-to-date information; and

(iv) validate the effectiveness of the awareness and training programme on a regular basis.

PART IX – REPORTING REQUIREMENTS

95. Financial institutions shall submit to the Bank the findings of all audits, assessments and testing exercises together with the remediation plan within 90 days from the date of completion of the respective exercise.

96. Financial institutions shall report cyber and technology events and incidents to the Bank in such manner and format prescribed by the Bank.

97. Financial institutions shall share cyber and technology threat intelligence information with the Bank in such manner and format prescribed by the Bank.

PART X - TRANSITIONAL ARRANGEMENTS

98. Financial institutions shall assess their compliance with the standards set out in this guideline and identify gaps vis-à-vis their current practices, if any.

99. Financial institutions shall address gaps identified with respect to critical processes, functions, systems, services, infrastructures and other assets at the earliest.

100. Financial institutions shall submit to the Bank a report on the findings of penetration testing and vulnerability assessments on critical systems, services, infrastructures and other assets conducted by independent specialists together with the remediation plan by end-November 2023.

101. Financial institutions shall submit to the Bank a board-approved gap analysis report against the requirements of this guideline together with a remediation plan covering the identified gaps and the findings of the penetration testing and vulnerability assessments, with timelines and milestones by end-January 2024.

102. Financial institutions shall take necessary measures to fully comply with all provisions of this guideline by end-June 2024.

103. Financial institutions shall ensure that their cyber and technology risk management framework is duly audited by an external independent assessor and submit the report to the Bank by end-November 2024. The report should include an assessment on the compliance of the financial institution with the provisions of this guideline, the effectiveness of its cyber and technology risk management framework and its maturity against a set of relevant external benchmarks.

Bank of Mauritius
29 May 2023