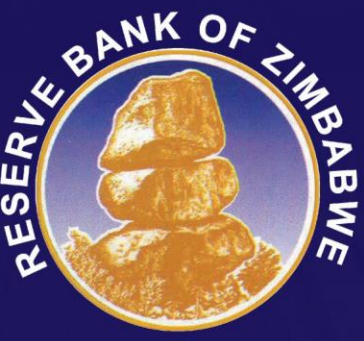

CYBERSECURITY AND RESILIENCE GUIDELINE

Current Version	
Revised Title	Cybersecurity and Resilience Guideline
Issue Date	August 2025
Version No.	02
Previous Version	
Previous Title	Risk Based Cybersecurity Guideline
Issue Date	April 2021
Version No.	01

Table of Contents

1. INTRODUCTION

1.1 Advancements in technology and telecommunications in the financial sector are driving enhanced efficiency, operational improvements, innovation as well as security and risk management.

1.2 The technological revolution also opens up the window for new types of risks and threats for players in the financial services sector.

1.3 The Reserve Bank has enhanced its Risk Based Cybersecurity Framework initially issued in April 2021 to provide updated guidance to the financial sector players to manage cybersecurity risks effectively, to ensure and secure technology systems in a manner which leads to a safe and sound digital environment for the sector.

1.4 The revised guideline aims to:

a) Enhance cybersecurity and resilience by guiding regulated institutions in identifying, managing, and mitigating cyber risks.

b) Align with global standards and operational resilience principles for robust cybersecurity practices.

c) Strengthen operational resilience through proactive risk management, continuous monitoring, and effective incident response.

d) Ensure regulatory compliance by providing a structured approach to meeting cybersecurity requirements, and

e) Promote a risk-based approach by requiring institutions to tailor cybersecurity strategies to their unique risks and operations.

1.5 The guideline covers:

a) Cybersecurity governance, roles, responsibilities, and oversight.

b) Risk assessment and threat intelligence, ensuring continuous monitoring of emerging threats.

c) Operational resilience, enabling institutions to prevent, detect, respond, and recover from cyber incidents.

d) Security controls, including encryption, authentication, and network protection.

e) Incident response and recovery, ensuring swift containment and mitigation of cyber threats.

f) Third-party risk management, addressing cybersecurity risks in vendor and supply chain relationships.

g) Legal and regulatory compliance requirements and best practices.

h) Cybersecurity awareness, fostering a strong security culture through training and capacity building.

1.6 **Appendix 1** of the Guideline provides a glossary of technical terms to enhance comprehension and clarity for the regulated institutions, while **Appendix 2** is an alphabetical list of abbreviations.

1.7 **Appendix 3** presents the Cyber Resilience Reporting Templates which should be submitted to the Reserve Bank regularly or on an ad-hoc basis. **Appendix 4** is an outline of the baseline guidance on minimum requirements for conducting a Cyber Resilience Self-Assessment.

1.8 The Guideline concludes with a list of **References** acknowledging the sources of information, standards and policies that have been included in this Guideline.

2. LEGAL AUTHORITY AND APPLICATION

Authorisation

2.1 The Cybersecurity Guideline is issued pursuant to the Banking Act (Chapter 24:20), Microfinance Act (Chapter 24:30) and the National Payment Systems Act (Chapter 24:23).

Application

2.2 This guideline applies to all banking institutions, non-bank financial institutions, controlling companies, payment system providers and other entities, regulated in terms of the laws and regulations administered by the Reserve Bank, herein referred to as "regulated institutions".

2.3 All regulated institutions are expected to maintain cyber security systems reflective of the standards set out in this guideline in a manner commensurate with the nature, size, and complexity of their operations.

Responsibility

2.4 The Reserve Bank will assess implementation of this guideline while regulated institutions are responsible for adopting and implementation.

2.5 The Reserve Bank will also review the institutions' policies on an on-going basis to assess their appropriateness and adequacy in line with the practices contained in the cyber resilience guidance principles.

2.6 Regulated institutions are required to enhance their risk management policies, processes and procedures on an ongoing basis.

3. CYBERSECURITY GOVERNANCE AND OVERSIGHT

3.1 Regulated institutions should establish governance structures to formulate, implement and oversee an effective cybersecurity policy that enables them to identify, protect, respond, detect, adapt and recover timeously without compromising stability of the financial sector ecosystem.

3.2 To ensure accountability, an institution should define clear roles and responsibilities for cybersecurity personnel, including:

a. Board of Directors & Executive Management – Oversight of cybersecurity strategy, approving key policies, and ensuring adequate funding.

b. Chief Information Security Officer (CISO) – Leading cybersecurity initiatives, ensuring compliance, and implementing security frameworks.

c. IT & Security Teams – Implementing cybersecurity controls, monitoring threats, and responding to incidents.

d. Business Units – Ensuring compliance with cybersecurity policies in daily operations.

e. All Employees – Undergoing regular cybersecurity training to recognise and prevent cyber threats.

A. Board of Directors

3.3 The ultimate responsibility for cybersecurity rests with the board of the institution and includes adopting and improving the organisational governance framework for cybersecurity.

3.4 The board may delegate primary oversight activity to an existing committee (e.g. the risk management committee) or a new committee (e.g. a cyber-resilience committee)

3.5 The Board of Directors play a critical role in cybersecurity by providing oversight, ensuring adequate risk management, and fostering a culture of security within the organisation, ultimately protecting stakeholders and the regulated institution’s reputation.

3.6 The board should ensure that it has a comprehensive understanding of the institution's cyber risk environment. This can be acquired through the expertise of in-house staff members or independent external experts.

3.7 The Board of Directors have overall responsibility for:

a. **Oversight and guidance:** Board members should ensure that executives and their teams set a high standard for cybersecurity, providing guidance and direction on cybersecurity strategy and risk management.

b. **Risk management:** The board is responsible for ensuring that cybersecurity risks are identified, evaluated, and mitigated appropriately, aligning with the regulated institution's overall risk appetite.

c. **Compliance and legal responsibilities:** Boards must understand and ensure compliance with relevant cybersecurity laws, regulations, and industry standards, as they are increasingly held accountable for cybersecurity failures.

d. **Accountability and transparency:** Boards need to clearly assign cybersecurity responsibilities and ensure that management has established procedures for incident response and disclosure.

e. **Monitoring and reporting:** The board should regularly review cybersecurity performance, monitor the effectiveness of security controls, and receive reports on the status of the cybersecurity program.

f. **Culture of security:** Boards should promote a culture of cybersecurity awareness and responsibility throughout the organisation, ensuring that all employees understand their role in protecting the institution's data and systems.

g. **Expertise and training:** Boards should ensure that management staff have the necessary cybersecurity knowledge and expertise to effectively oversee the institution's cybersecurity program.

h. **Tabletop exercises:** The board or committee overseeing cyber issues should ensure that management has conducted tabletop exercises to test and assess the institution's incident response and its processes for disclosures.

3.8 The board of an institution should appoint a **Chief Information Security Officer** (CISO) **or a similarly senior executive** who has the necessary skills and experience to be responsible for the institution's cyber resilience strategy and operational framework.

3.9 The board of an institution is also responsible for developing the institution's cyber risk appetite and tolerance to help them determine the appropriate cyber resilience strategy and framework.

3.10 The board should be responsible for approving the institution's cyber resilience framework and strategy. It should also regularly monitor the implementation status of the program and ensure that the institution's policies and procedures are being followed properly.

3.11 The board is also responsible for ensuring that a formal, independent cyber-resilience review of the institution is carried out at least annually.

B. Senior Management

3.12 Senior management should play a crucial role by setting the tone, establishing policies, allocating resources, and fostering a culture of security, ensuring compliance and accountability at all levels. They are responsible for protecting the institution's digital assets and ensuring compliance with legal and regulatory requirements as further outlined below.

a. **Strategic Planning and Vision:** Senior management, including the CISO, are responsible for developing and implementing a comprehensive cybersecurity strategy that aligns with the organisation's overall business goals.

b. **Policy Development and Enforcement:** They must ensure that cybersecurity policies are in place and enforced, covering areas such as data protection, access control, and incident response. These should be reviewed at least annually and should also be made available for review by external auditors, the Reserve Bank supervisors or any other relevant regulatory bodies as and when required.

c. **Clearly Define Roles and Responsibilities:** The roles and responsibilities of all management and oversight functions (including lines of defence) should be clearly defined as well as committees established for the purposes of exercising oversight of cyber risks.

d. **Independent Information Security Function**: Ensure that an information security function with adequate resources, appropriate authority, and access to the Board is established where applicable. This function must be responsible for all cyber and information security issues within the regulated institution. Ensure that the governance and oversight of the information security function is independent from operations to ensure adequate segregation of duties and avoid any potential conflict of interest.

e. **Resource Allocation and Budgeting:** Senior management play a vital role in allocating sufficient resources, including funding and personnel, to support cybersecurity initiatives.

f. **Risk Management and Compliance**: Senior management must understand and manage cybersecurity risks, ensuring compliance with relevant regulations and industry standards.

g. **Incident Response and Crisis Management:** Senior management are responsible for overseeing incident response and crisis management efforts including reporting in the event of a security breach.

h. **Fostering a Security Culture:** Senior management must promote a culture of security awareness and accountability throughout the institution, encouraging employees to prioritise cybersecurity best practices.

i. **Stakeholder Engagement:** Senior management must communicate effectively with stakeholders, including board members, investors, and customers, about cybersecurity risks and mitigation efforts.

j. **Third Party Management**: Senior management should ensure that roles and responsibilities for security are clearly defined in the contract or Service Level Agreement with third-party service providers, as further outlined in Section 5.

k. **Staying up-to-date**: Senior management must stay informed about the latest cybersecurity threats and trends, ensuring that the organisation's security posture remains strong.

l. **Accountability and Oversight:** Senior management is ultimately accountable to the Board for the institution's cybersecurity performance and must provide oversight to ensure that security programs are effective.

m. **Training and Education:** Senior management must ensure that employees receive adequate cybersecurity training and education to help them recognise and respond to potential threats.

3.13 The senior management should also regularly update the board on the status of the regulated institution's cyber resilience program and strategy. They should also keep the board informed about the institution's future resource allocation plans. This will help ensure that the organisation's cyber risk appetite and tolerance are maintained.

C. Information and Cyber Security Management

3.14 The regulated institution must institutionalise the cybersecurity function in a way that ensures appropriate level of independency of any other role that might conflict with cybersecurity program and objectives, including reporting arrangements, budget and resources. Cybersecurity function shall:

a. Develop and maintain the cybersecurity program including cyber risk management processes, as well as cybersecurity-related strategy, policy, standards, procedures, guidelines and baselines, key risk indicators and key performance indicators for the cybersecurity program.

b. Develop the approach for engaging cybersecurity function in the organisation processes at all levels.

c. Manage cyber risk assessments, propose mitigation controls and procedures in a business context, and define cybersecurity requirements for new and on-going projects and business activities, as well as managing the process of information and system classification.

d. Manage the implementation of the cybersecurity program.

e. Assess the adequacy of controls and approve exceptions considering the stated cyber risk appetite and enforced regulations.

f. Monitor, analyse and communicate information on security alerts and events.

g. Establish and communicate security incident management processes, and oversee incident response, handling and escalation procedures.

h. Gather, analyse and utilise threat intelligence information.

i. Examine and make recommendations, in the areas of cybersecurity in the institution, to be reviewed and approved by the board.

j. Measure the performance of the cybersecurity program and measure the defined key risk indicators.

k. Develop measuring and monitoring process for the compliance with cybersecurity policy, standards and procedures.

l. Develop and conduct cybersecurity awareness programs and periodically measure the programs' effectiveness.

m. Periodically or on a need basis update board of directors and the committee about the status of cybersecurity program and initiatives.

3.15 Based on the size of the institution, cybersecurity responsibilities (not accountability) can be assigned to different – but dedicated – functional units positioned properly in the organisational structure.

D. ICT Management

3.16 In the context of cybersecurity, ICT function is responsible for:

a. Implementing policies, controls, standards and guidelines emanating from cybersecurity program over systems and services.

b. Committing to acceptable risk levels and limits, and informing Information Security Management about any raised risks, gaps, and breaches related to approved and acceptable risk limits and levels, or any policy violation.

c. Remediating security vulnerabilities in timeframes according to their criticalities.

d. Maintaining and monitoring security tools and technologies. This includes regular update and maintenance for the applied security measures.

e. Committing to security incident response program and maintaining a well-defined and documented plan of actions to put into place if a security incident does occur.

E. Cybersecurity Strategy and Policies

3.17 An institution should develop a comprehensive cybersecurity strategy and policies that adequately addresses its vulnerabilities and threats.

Cybersecurity Strategy

3.18 The institution should have a comprehensive cybersecurity strategy that is aligned with its various business objectives and stakeholder requirements. It should also ensure that its strategy is aligned with its risk tolerance and appetite and other related risk management strategies.

3.19 The institution's cybersecurity strategy should be regularly updated, at least annually, to ensure that it can continue operating effectively in the current cyber risk environment.

3.20 The cybersecurity strategy, at a minimum, should outline:

a. The importance of cybersecurity to the institution;

b. High level requirements of the institution’s stakeholders;

c. The institution’s cyber resilience vision, mission and objectives;

d. The cyber risk appetite as well as cyber resilience targets and implementation plan;

e. The necessary resources and technology to manage and implement cyber resilience initiatives;

f. Business continuity and disaster recovery;

g. Technology and security controls;

h. Regulatory compliance; and

i. Communication and stakeholder management.

Cybersecurity Policy

3.21 In order to address the need for the entire institution to contribute to a cyber-safe environment, the Cyber Security Policy should be distinct and separate from

the broader IT policy / IS Security policy so that it can highlight the risks from cyber threats and the measures to address / mitigate these risks.

3.22 The size, systems, technological complexity, digital products, stakeholders and threat perception vary across institutions and hence it is important to identify the inherent risks and the controls in place to adopt an appropriate cyber-security framework.

3.23 A regulated institution's cybersecurity policy should be a structured document that provides actionable guidelines on cyber risk management. At a minimum it must:

a. Outline how the institution sets its risk tolerance and cyber resilience objectives and state how the institution identifies, mitigates and manages its cyber risk to support its objectives;

b. Provide guidance related to governance, capability building, information sharing and third-party management;

c. Be designed using leading international and national standards and guidelines as a benchmark such as:

   i. ISO/IEC 27001 (Information Security Management Systems).

   ii. Basel Committee on Banking Supervision (BCBS) Cyber Guidelines.

   iii. NIST Cybersecurity Framework.

   iv. Bank of International Settlements Committee on Payments and Market Infrastructures.

d. Incorporate monitoring metrics coupled with reporting and trend analysis:

   i. Define procedures for real-time monitoring of cyber threats.

   ii. Establish reporting structures for security incidents and vulnerabilities.

   iii. Depending on the level of inherent risks, identify their riskiness as low, moderate, high and very high or adopt any other similar categorisation.

e. Be consistent with the institution's enterprise risk management framework.

   i. Ensure cybersecurity is integrated into broader risk management frameworks.

   ii. Define escalation procedures for reporting cyber incidents to executive management, the board, regulators, customers and any other key and relevant stakeholders.

F. Cybersecurity Audits & Continuous Improvement

3.24 An effective cybersecurity audit process (internal and external) should be carried out to help monitor and measure the effectiveness of the organisation's strategy and policies.

3.25 Regulated institutions must:

a) Establish robust audit mechanisms to evaluate the effectiveness of cybersecurity strategies and policies.

b) Conduct internal cybersecurity audits at least twice a year, focusing on policy adherence, risk assessments, and security gaps.

c) Engage external cybersecurity firms or regulators for independent security assessments at least annually.

d) Implement continuous improvement practices, updating policies based on audit findings, new threats, and industry trends.

G. Culture and Awareness

3.26 The regulated institution should have a culture that acknowledges the responsibilities of its staff at all levels in ensuring its cyber resilience.

3.27 This culture should be communicated through effective internal communication channels, sharing information about the institution’s cyber resilience strategy and procedures.

3.28 A cyber resilient institution should have a strong culture that promotes continuous improvement and the development of a resilient business environment.

3.29 An institution should also have a process that allows it to gather and analyse cyber threat intelligence. This process should be used to enhance the company's situational awareness.

3.30 A comprehensive program should also be created and maintained to provide continuous training for employees on cyber resilience.

3.31 The training should cover current cyber threats and attack tactics, as well as appropriate response procedures relevant for all employees' responsibilities.

4. CYBERSECURITY RISK MANAGEMENT

4.1 A regulated institution's cyber resilience strategy should at a minimum outline five (5) primary risk management categories to ensure effective management of cyber risk on an on-going basis.

4.2 The cybersecurity risk management functions are (i) **governance** (covered in section 3 above), (ii) **identification**, (iii) **protection**, (iv) **detection**, and (v) **response and recovery**.

A. Identification and risk assessment

4.3 A regulated institution must identify which of its critical operations and supporting information assets should, in order of priority (criticality and sensitivity), be protected against compromise. The institution should understand its internal situation and external dependencies to effectively respond to potential cyber threats that might occur.

4.4 To this end, the regulated institution should know its information assets and understand its processes, procedures, systems and all dependencies in order to guide the prioritisation of its protective, detective and response efforts in order to strengthen its overall cyber resilience posture.

4.5 At a minimum, a regulated institution should:

a) identify and document all its critical functions, key roles, processes and information assets that support those functions, including those managed by third party service providers and update this information on a regular basis;

b) maintain an up-to-date inventory of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections. The regulated institution should integrate identification efforts with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its inventory;

c) have an enterprise risk management framework to identify risks and conduct risk assessments on a regular basis;

d) create and maintain a simplified network map of resources with an associated plan addressing internet protocols which locate routing and security devices and servers supporting the regulated institution's critical functions, and which identify links with the outside world;

e) conduct risk assessments before deploying new and/or updated technologies, products, services and connections to identify potential threats and vulnerabilities;

f) update its risk assessment in case new information affecting cybersecurity risks is identified (e.g. a new threat, vulnerability, adverse test result,

hardware change, software change or configuration change). The results of the risk assessments should feed into the cyber resilience strategy and framework;

g) have and maintain a fully comprehensive active directory of all individual and system accounts (especially privileged and remote access accounts) so that they can be aware of the access rights to information assets and their supporting systems. The regulated institution should review and update this inventory on a regular basis;

h) use automated tools (e.g. a centralised asset inventory management (AIM) tool) that enable it to support the identification and classification of the critical functions, processes, information assets and interconnections. The regulated institution should ensure that the inventory is updated accurately and that these changes are shared with the relevant staff in a timely manner;

i) use automated tools (e.g. a centralised identity and access management (IAM) tool) that enable it to support the identification and classification process of roles, user profiles and individual and system credentials, and ensure that these are updated accurately and that relevant staff are informed of the changes in a timely manner;

j) maintain up-to-date and complete maps of network resources, interconnections and dependencies, and data flows with other information assets, including the connections to business partners, internet-facing services, cloud services and any other third-party systems. It should use these maps to undertake risk assessments of key dependencies and apply appropriate risk controls, when necessary;

k) update its inventory to address new, relocated, repurposed and sunset information assets, on a regular basis or when these changes occur;

l) use automated feeds from above (e.g. from AIM and IAM tools), in order to identify emerging risks, update its risk assessments in a timely manner and take the necessary mitigating actions in line with the regulated institution's risk tolerance; and

m) identify the cyber risks that it bears from or poses to entities in its ecosystem and coordinate with relevant entities, as appropriate. This may involve identifying common vulnerabilities and threats, and taking appropriate measures collectively to address such risks, with the objective of improving the ecosystem's overall resilience.

B. Protection

4.6 The protection function entails appropriate safeguards to ensure delivery of critical infrastructure services and supports the ability to limit or contain the impact of a potential cybersecurity event.

4.7 Regulated institutions must have effective security controls and system as well as process design that protect the confidentiality, integrity and availability of its assets and services, including key roles, processes, systems, information assets, interconnections, third party providers.

Control Implementation and Design

4.8 A regulated institution must implement appropriate and effective cyber resilience capabilities and cybersecurity practices to prevent, limit or contain the impact of a potential cyber event. At a minimum, a regulated institution should:

a) implement a comprehensive and appropriate set of security controls that will allow it to achieve the security objectives which include the following:

   i. the continuity and availability of its information systems;

   ii. the integrity of the information stored in its information systems, while both in use and transit;

   iii. the protection, integrity, confidentiality and availability of data while at rest, in use and in transit; and

   iv. conformity to applicable laws, regulations and standards.

b) implement controls based on the identification of its critical functions, key roles, processes, information assets, third-party service providers and interconnections, as per the risk assessment in the identification phase;

c) develop its security controls to address cybersecurity and related physical security and people security. The controls should be designed according to the threat landscape, prioritised in accordance with the risks facing the regulated institution (risk-based security controls) and aligned to its business objectives;

d) assess the effectiveness of its security controls regularly to adapt them to its evolving threat landscape. The controls should be monitored and audited regularly to ensure that they remain effective and have been applied to all assets where they might be needed;

e) capture security requirements alongside system and process requirements when designing, developing and acquiring systems and processes, in order to identify the security controls necessary for protecting its systems, processes and data, at the earliest possible stage;

f) apply a defence-in-depth strategy, in line with a risk-based approach, i.e. it should implement multiple independent security controls so that if one control fails or a vulnerability is exploited, alternative controls will be able to protect targeted assets and/or processes;

g) develop and implement a bespoke information security management system (ISMS), which could be based on a combination of well-recognised international standards (e.g. ISO 27001, ISO 20000-1 and ISO 27103, etc.), in order to establish, implement, operate, continuously monitor, review, maintain and improve a comprehensive cybersecurity control framework;

h) consider cyber resilience at the earliest stage of system design, development and acquisition, as well as throughout the system development life cycle, so that vulnerabilities in software and hardware are minimised and security controls are incorporated into systems and processes from their inception;

i) adopt a bespoke system development life cycle (SDLC) methodology that embeds the resilience-by-design approach when designing, building, acquiring or modifying its systems, processes and products;

j) frequently review ISMS, using certification, audits or other relevant forms of assurance; and

k) develop processes and procedures and explore potential technologies to constantly adjust and refine its security countermeasures (controls).

Network & Infrastructure Management

4.9 A regulated institution must at a minimum:

a) establish a secure boundary that protects its network infrastructure (using tools such as a router, firewall, Intrusion Prevention System (IPS) or Intrusion Detection System (IDS), Virtual Private Network (VPN), Demilitarised Zone (DMZ) or Proxies etc.);

b) reinforce its network infrastructure and information systems using recognised industry security standards. Changes to system configurations should be strictly controlled and monitored and programmes that can alter or override system configuration should be restricted;

c) install network security devices to secure the network between the regulated institution and the internet, as well as connections with third-party service providers;

d) deploy network intrusion detection or prevention systems to detect and block malicious traffic;

e) review its network architecture, including the network security design; as well as systems and network interconnections on a periodic basis to identify potential vulnerabilities;

f) define and implement procedures that limit, lock and terminate system and remote sessions after a predefined period of inactivity and predefined conditions are met;

g) implement network access controls to detect and prevent unauthorised devices from connecting to its network. Network access control rules in network devices must be reviewed on a regular basis to ensure they remain up-to date;

h) consider isolating internet web browsing activities from its endpoint devices through the use of physical or logical segregation, or implement equivalent controls, to reduce exposure of its IT systems to cyber-attacks;

i) encrypt remote connections to prevent data leakages through network sniffing and eavesdropping;

j) have policies and controls that prevent users from installing unauthorised applications;

k) scan its legacy technologies regularly to identify potential vulnerabilities and seek upgrade opportunities. Controls and additional defence layers should be implemented and tested in order to protect unsupported or vulnerable systems;

l) employ automated mechanisms to help maintain an up-to-date, complete, accurate and readily available baseline of system and security configurations for the information system and system components;

m) isolate affected information assets in the case of an adverse event; and

n) seek to implement cyber deception capabilities and techniques that enable it to lure the attacker and trap it in a controlled environment where all activities can be contained and analysed, allowing the regulated institution to gain vital threat intelligence that will help to improve its protection controls.

Logical and Physical Security Management

4.10 A regulated institution should:

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

b) establish policies, procedures and controls that address access privileges and how that access should be administered. Administration rights on systems

should be strictly limited to operational needs. Procedures should be in place for a periodic review of all access rights;

c) establish and administer user accounts in accordance with a role-based access control scheme that organises allowed information system access rights and privileges into roles. Role assignments should be reviewed regularly by appropriate staff (e.g. management and system owners) in order to take appropriate action when privileged role assignments are no longer appropriate;

d) establish processes to manage the creation, modification or deletion of user access rights. Such actions should be submitted to and approved by appropriate staff, and should be recorded for review if necessary;

e) implement specific procedures to allocate privileged access on a need-to-use or an event-by-event basis. Administrators should have two types of accounts: one for general purpose and another to carry out their administrative tasks. The use of **privileged accounts** should be tightly monitored and controlled. The use of **generic accounts** for administration purpose should be strictly limited and traced. Whenever possible, user and administrator accounts should be nominative and clearly identifiable (e.g. using dedicated taxonomy for usernames, which ensures that the positions and roles are not apparent);

f) have a dedicated policy that covers all the characteristics of its **authentication mechanisms** (e.g. password, smart cards and biometrics, etc.) and is in line with relevant standards (e.g. NIST-800-63). Default authentication settings (e.g. passwords and unnecessary default accounts) should be deactivated, changed or removed before systems, software and/or services go live;

g) develop appropriate controls (e.g. encryption, authentication and access control) to protect data at rest, in use and in transit. The controls should be commensurate to the criticality and the sensitivity of the data held, used or being transmitted, as per the risk assessment conducted in the identification phase;

h) have dedicated controls to prevent unauthorised access to cryptographic keys. Dedicated policy and procedures should be defined for the management of and access to cryptographic materials;

i) implement controls to prevent unauthorised privileged escalation (e.g. technical controls that trigger automated notification to appropriate staff in the case of changes to user access profiles);

j) encrypt data as a result of its data classification and risk assessment processes. The regulated institution should also use **encryption and**

general cryptographic controls in line with recognised standards and processes, which cover aspects such as algorithm, key length and key generation, etc.;

k) implement automated mechanisms to support the management of information system access accounts, including implementing security controls embedded in the information system, allowing it to automatically disable and/or remove inactive, temporary and emergency accounts after a predefined period of time;

l) establish strong governance on identity and access management enforced by the use of dedicated tools such as Identity and Access Management (IAM), in an integrated way, ensuring all systems update each other consistently;

m) seek to use an **attribute-based access contro**l paradigm that allows it to manage access to its IT environment contextually and dynamically;

n) employ automated mechanisms that allow account creation, modification, enabling, disabling and removal actions to be monitored;

o) employ automated auditing and continuous monitoring mechanisms to detect anomalous or potentially malicious user activity. The system should generate alerts and notify appropriate staff in real time when suspicious behaviour is detected; and

p) implement adaptive access controls that dynamically adjust user permissions based on contextual risk factors (e.g. time of access, device, location, or behavioural anomalies) to proactively prevent unauthorised activity or damage

Change and Patch Management

4.11 The changes to information systems include modifying hardware, software or firmware components and system security configuration settings.

4.12 A regulated institution should have controls with regards change and patch management which include the following:

a) policies, procedures and controls for change management, including criteria for prioritising and classifying the changes (e.g. normal vs. emergency change).

b) Prior to any change, the regulated institution should ensure that the change request is:

i. reviewed to ensure that it meets business needs;

ii. categorised and assessed for identifying potential risks and to ensure that it will not negatively impact confidentiality, integrity and availability, as well as the regulated institution's systems and data; and

iii. approved before it is implemented by the appropriate level of management.

c) ensure that the cybersecurity team is involved throughout the life cycle of the change management process, as appropriate;

d) put necessary procedures in place (e.g. code review and unit testing, etc.), which guarantee that changes are implemented correctly and efficiently;

e) test, validate and document changes to the information system before implementing them into production (integration tests, non-regression tests and user acceptance tests, etc.);

f) have processes to identify, assess and approve genuine emergency changes;

g) post-implementation reviews should be conducted to validate that emergency procedures were appropriately followed and to determine the impact of the emergency change;

h) have a comprehensive **patch management** policy and processes that include:

i. maintaining current knowledge of available patches;

ii. identifying appropriate patches for particular systems and analysing impacts if installed;

iii. assuring that patches are installed properly (e.g. by applying the four-eyes principle) and tested prior to and monitored after installation; and

iv. documenting all associated procedures, such as specific configurations required. The policies, procedures and controls must make use of the information AIM[1] process described in the identification phase that provides information on the installed programs and binaries.

i) consider using standardised configuration of IT resources to facilitate its patch management process;

j) ensure that the installations of new patches have prior approval from the appropriate level of management;

k) have in place necessary procedures for recovering quickly when changes or patches fail. Any changes to the production environment must have an associated fall-back plan, when applicable;

[1] Asset Inventory Management

l) have policies and procedures to prohibit changes and patch installation to the information system that have not been pre-approved;

m) establish its change management process based on well-established and industry-recognised standards and best practices (e.g. the information technology infrastructure library);

n) consider automating patch management process when possible to guarantee that all systems remain consistently up to date;

o) consider building a segregated or separate environment that mirrors the production environment, allowing rapid testing and changes and patches to be implemented, and providing for rapid fall-back when needed; and

p) implement automated mechanisms that prohibit changes and patches from being installed on the information system that have not been pre-approved.

People Management - Human Resources Security

4.13 The regulated institution should embed cybersecurity at each stage of the employment life cycle, specifying security-related actions required during the induction of each employee and their ongoing management, and upon the termination of their employment. At a minimum, the following cybersecurity controls should be observed.

4.14 ***Prior to Employment…***

a) carry out background security checks on all candidates (employees and/or contractors) commensurate to their future role and depending on the criticality of the assets and information they might have access to in order to fulfil their duty; and

b) responsibilities for cybersecurity should be clearly stated in the contractual agreement.

4.15 ***During Employment…***

a) ensure that employees and contractors comply with established policies, procedures and controls;

b) ensure that all access rights that are related to his/her previous position and are not necessary for his/her new responsibilities are revoked in due time, when an employee is changing responsibilities;

c) employees in sensitive positions (e.g. those who change to roles requiring privileged access to critical systems or who become high-risk staff) should be pre-screened;

d) Empower staff within the organisation through ***awareness and training*** including role based and privileged user training;

4.16 ***Termination of Employment…***

a) establish procedures to revoke all departing employees' access rights from the information assets in a timely manner; and

b) staff should be required to return all assets that belong to the regulated institution, including important documentation (e.g. related to business processes, technical procedures and contact details), equipment, software and authentication hardware, etc.

4.17 In addition, human resources security controls should:

a) establish policies, procedures and controls for granting or revoking employees physical and logical access to its systems based on job responsibilities, principles of least privilege and segregation of duties. Procedures for regularly reviewing such access should be in place;

b) establish capabilities, including people, processes and technologies to monitor privileged users' activity and access to critical systems in order to identify and deter anomalous behaviour and notify appropriate staff;

c) implement mechanisms that trigger automatic notifications to be sent to staff in charge of granting or revoking access to the information system upon change to employment status;

d) implement automatic mechanisms to grant or revoke staff access to information system upon change to employment status; and

e) monitor and analyse pattern behaviour (e.g. network use patterns, work hours and known devices, etc.) to identify anomalous activities and evaluate the implementation of innovative solutions (e.g. data analytics, machine learning and artificial intelligence, etc.) to support detection and response to insider threat activity in real time.

C. Detection

4.18 The detect function defines the appropriate activities to identify the occurrence of a cybersecurity event and enables timely discovery of cybersecurity events.

4.19 A regulated institution's ability to recognise signs of a potential cyber incident, or detect that an actual breach has taken place, is essential to strong cyber resilience. Early detection provides a regulated institution with useful lead time to mount appropriate countermeasures against a potential breach and allows proactive containment of actual breaches.

4.20 Based on the risk assessment performed in the identification phase, the regulated institution should define, consider and document the baseline profile

of system activities to help detect deviation from the baseline (e.g. anomalous activities and events).

4.21 In addition, to ensure that cyber incidents are timeously detected, a regulated institution should:

a) develop the appropriate capabilities, including the people, processes and technology, to monitor and detect anomalous activities and events, by setting appropriate criteria, parameters and triggers to enable alerts;

b) configure IT system events or alerts to provide an early indication of issues that may affect its performance and security;

c) have capabilities to monitor user activity, exceptions, cybersecurity events, connections, external service providers, devices and software;

d) actively monitor events or alerts so that prompt measures can be taken to address the issues early;

e) analyse the information collected and use it to further enhance its detection and monitoring capabilities and incident response process;

f) ensure that its detection capabilities, baseline profile of system activities and the criteria, parameters and triggers are periodically reviewed, tested and updated appropriately, in a controlled and authorised manner;

g) ensure that its relevant staff (employees and/or contractors) are trained to be able to identify and report anomalous activity and events;

h) build multi-layered detection controls covering people, processes and technology which support attack detection and isolation of infected points;

i) ensure that detection capabilities are informed by threat or vulnerability information, which can be collected from different sources and providers;

j) define alert thresholds for monitoring and detection systems in order to trigger and facilitate the incident response process. A regulated institution's monitoring and detection capabilities should support information collection for the forensic investigation;

k) develop and implement automated mechanisms (e.g. a security information and event management (SIEM) system), which correlates all the network and system alerts and any other anomalous activity across its business units in order to detect multifaceted attacks (e.g. simultaneous account takeover or a distributed denial of service (DDoS) attack);

l) have a process to collect, centralise and correlate event information from multiple sources and log analysis to continuously monitor the IT environment (e.g. databases, servers and end points, etc.) and detect anomalous activities and events on the network across business units;

m) have processes in place to monitor activities that are not in line with security policy and might lead to data theft, integrity compromise or destruction;

n) have the capabilities, in collaboration with other stakeholders, to detect cyber events and adapt security controls swiftly. Such events may include attempted infiltration, movement of an attacker across systems, exploitation of vulnerabilities, unlawful access to systems and exfiltration of information or data;

o) continuously monitor connections among information assets and cyber risk levels throughout the information assets' life cycles, and store and analyse these data. The information gathered this way should enable the regulated institution to support timely responses to cyber threats (including insider threats) or vulnerabilities and investigation of anomalous activities;

p) continuously monitor and inspect the network traffic, including remote connections, and end point configuration and activity to identify potential vulnerabilities or anomalous events in a timely manner. Compare the network traffic and the end point configuration with the expected traffic and configuration baseline profile and data flows;

q) use multiple external sources of intelligence, correlated log analysis, alerts, traffic flows, and geopolitical events to predict potential future attacks and attack trends, and proactively take the appropriate measures to improve its cyber resilience capabilities;

r) develop threat detection capabilities which can detect both known and unknown threats, with a proactive identification of vulnerabilities, state-of-the art threat detection and correlation between vulnerabilities and threats;

s) should seek to continuously explore new technologies and techniques inhibiting lateral movement (e.g. deception mechanisms) which trigger alerts and inform the regulated institution of potential malicious activity when accessed, and.

t) establish a process for timely escalation to relevant stakeholders regarding suspicious or anomalous system activities or user behaviour.

Cyber Threat Intelligence

4.22 A regulated institution should identify cyber threats that could materially affect its ability to perform or provide services as expected, or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its ecosystem.

4.23 At a minimum, the regulated institution should:

a) have capabilities in place to gather cyber threat information from internal and external sources (e.g. application, system and network logs; security products such as firewalls and IDSs; trusted threat intelligence providers; and publicly available information);

b) belong or subscribe to a threat and vulnerability information-sharing source and/or ISAC that provides information on cyber threats and vulnerabilities. Cyber threat information gathered by the institution should include analysis of tactics, techniques and procedures (TTPs) of real-life attackers, their modus operandi and information on geopolitical developments that may trigger cyber-attacks on any entity within the institution's ecosystem;

c) have the capabilities to analyse the cyber threat information gathered from different sources, while considering the business and technical characteristics of the regulated institution, in order to:

   i) determine the motivation and capabilities of threat actors (including their TTPs) and the extent to which the regulated institution is at risk of a targeted attack from them;

   ii) assess the risk of technical vulnerabilities in operating systems, applications and other software, which could be exploited to perform attacks on the regulated institution; and

   iii) analyse cybersecurity incidents experienced by other institutions (where available), including types of incident and origin of attacks, target of attacks, preceding threat events and frequency of occurrence, and determine the potential risk these pose to the regulated institution.

d) analyse the information gathered above to produce relevant cyber threat intelligence, and continuously use it to assess and manage security threats and vulnerabilities for the purpose of implementing appropriate cybersecurity controls in its systems and, on a more general level, enhancing its cyber resilience framework and capabilities on an ongoing basis;

e) ensure that the gathering and analysis of cyber threat information and the production of cyber threat intelligence are reviewed and updated regularly;

f) ensure that cyber threat intelligence is made available to appropriate staff who are responsible for mitigating cyber risks at the strategic, tactical and operational levels within the regulated institution;

g) incorporate lessons learned from analysis of the cyber threat information into the employee training and awareness programmes;

h) continuously use cyber threat intelligence to anticipate, as much as possible, a cyber-attacker's capabilities, intentions and modus operandi, and subsequently possible future attacks;

i) develop a **cyber-threat risk dashboard**, which uses the cyber threat information and intelligence to outline, among other things:

   i) the most likely threat actors for the regulated institution;

   ii) the TTPs that may be used by such threat actors;

   iii) the likely vulnerabilities that may be exploited by such threat actors;

   iv) the likelihood of attack from such threat actors and the impact on the confidentiality, integrity and availability of the regulated institution's business processes and its reputation that could arise from such attacks;

   v) the impact of attacks already conducted by such threat actors on the ecosystem; and

   vi) the risk mitigation measures in place to manage a potential attack.

j) continuously review and update the cyber threat risk dashboard in the light of new threats and vulnerabilities;

k) include in the threat analysis, those threats which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. The regulated institution should review and update this analysis regularly;

l) ensure that the scope of cyber threat intelligence gathering includes the capability to gather and interpret information about relevant cyber threats arising from the institution's participants, service and utility providers and other regulated institutions, and to interpret this information in ways that allow the regulated institution to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards in its systems;

m) integrate and align cyber threat intelligence process with its **Security Operations Centre** (SOC). The regulated institution should use information gathered from its SOC to further enhance its cyber threat intelligence; and conversely, use its cyber threat intelligence to inform its SOC.

D. Response and Recovery

4.24 A regulated institution's ***business continuity*** arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data to mitigate the potentially systemic risks of failure.

Response and Recovery Plans

4.25 Regulated institutions should have **response and recovery plans** in place for when a cyber incident or breach occurs, and the plans should be aligned with its business continuity plans.

4.26 These plans which should be based on the identification and categorisation of its critical functions should include:

a) operating in a diminished capacity;

b) safe restoration of systems and services in the order of their relative priority;

c) recovery point objectives; and

d) recovery time objectives, commensurate to the entity's requirements and its systemic importance.

4.27 The plans should outline the internal and external stakeholders that must be notified of a cyber incident, when a notification must occur, and what information needs to be included in the notification.

4.28 The level of stakeholder engagement should be informed by the severity and impact of a cyber incident and should also outline the criteria for escalation within the entity, including to senior management and the board, based on the potential impact of the cyber incident.

4.29 An institution should have an internal system to classify cyber incidents into categories or tiers based on severity e.g. **critical incidents**, **major incidents** and **minor incidents.**

4.30 A regulated institution is required to report all cyber incidents to the Reserve Bank within a **period of 3 hours** or as soon as it becomes aware of the attack (**Appendix 3**). The institution's internal classification of an incident should be indicated in reports to the Reserve Bank.

4.31 The response and recovery plans should include clearly defined roles and responsibilities for all staff involved in cyber incident escalation, response and recovery, across all teams and departments within the entity.

4.32 Regulated institutions should utilise their process for triggering cyber incident alerts to ensure the right staff are aware of the incident or breach and have the most up-to-date information so that they can respond accordingly.

4.33 When formulating the response and recovery plans, a regulated institution should consider a wide range of different cyber incident scenarios, and in doing so conduct ***business impact analyses*** to assess how each scenario would impact the entity so that it can respond accordingly. The impact analyses should be conducted regularly and updated to reflect the ever-evolving cyber threat landscape that the entity faces.

4.34 Regulated institutions should establish systems' ***recovery time objectives*** and ***recovery point objectives*** that are aligned to its business resumption and system recovery priorities. The plan should include procedures to recover systems from various disaster scenarios, as well as the roles and responsibilities of relevant personnel in the recovery process.

4.35 The plans should be reviewed ***at least annually*** and updated when there are material changes to business operations, information assets or environmental factors.

4.36 During the recovery process, the regulated institution should follow the established ***disaster recovery plan*** that has been tested and approved by management and should avoid deviating from the plan as untested recovery measures could exacerbate the incident and prolong the recovery process.

4.37 In exceptional circumstances where untested recovery measures need to be used, the regulated institution should perform a risk assessment and ensure adequate controls are in place, as well as obtain approval from senior management.

4.38 Thus, the plans should allow regulated institutions to resume operations responsibly, while allowing for continued remediation by:

a) eliminating harmful remnants of the incident;

b) restoring systems and data to normal and confirming normal state;

c) identifying and mitigating all vulnerabilities that were exploited;

d) remediating vulnerabilities to prevent similar incidents; and

e) communicating appropriately internally and externally.

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

4.40 Regulated institutions should endeavour to operate from its disaster recovery, secondary or alternate site periodically to have the assurance that its infrastructure and systems at these sites are able to support business needs for an extended period when production systems fail.

Testing

4.41 Regulated institutions shall maintain a robust information security testing and vulnerability assessment framework to validate the effectiveness and resilience of cybersecurity controls. This framework must evolve to address emerging

threats and vulnerabilities identified through continuous threat monitoring and ICT risk assessments.

4.42 The framework shall include the following elements, applied in line with the institution's risk profile, size, and criticality of operations:

a) **Vulnerability Assessments (VA):** Regular automated and manual scans to detect known weaknesses, insecure configurations, and common web application vulnerabilities.

b) **Penetration Testing (PT):** Comprehensive testing of systems, networks, and applications to identify exploitable weaknesses, using **black-box**, **grey-box**, or **white-box** methods.

c) **Threat-Led Penetration Testing (Red Team Testing):** For institutions with critical functions or higher risk profiles, scenario-based testing shall simulate real-world advanced threats to assess the institution's ability to prevent, detect, respond to, and recover from sophisticated attacks.

4.43 Where applicable, regulated institutions shall conduct Red Team Testing, referencing recognised international frameworks such as:

a) TIBER-EU Framework;

b) CBEST Intelligence-Led Testing Framework;

c) GFMA TLPT Framework, and;

d) NIST SP 800-115 Framework.

4.44 The tests should:

a) Be based on up-to-date, relevant threat intelligence;

b) Emulate tactics, techniques, and procedures (TTPs) of real-life threat actors;

c) Assess not only preventive controls but also detective and response capabilities; and

d) Be conducted by qualified, independent testers with appropriate accreditation and experience.

4.45 At a minimum, all critical systems and internet-facing services shall undergo penetration testing at least **once every year**, and whenever significant changes or new threats emerge.

4.46 In particular, a regulated institutions should include API security testing as well as the cloud environment in their scope for critical systems. Further, the institution should engage certified testers with OSCP, CREST or other acceptable certifications.

4.47 Vulnerability assessments shall be conducted regularly to identify and address security weaknesses.

4.48 Red Team Testing shall be undertaken at a frequency aligned with the institution's risk profile, operational criticality, and supervisory expectations.

4.49 Testing shall be performed by suitably skilled and **independent testers** who are not involved in the development or operation of the controls being tested.

4.50 A formal **Testing Plan** and Rules of Engagement (RoE) must be documented and approved in advance to manage operational risks and safeguard data integrity.

4.51 The **scope of testing** must cover business logic, system functionality, access controls, and performance under realistic load and stress conditions. Dedicated, controlled environments shall be used for different test phases, with access strictly limited on a need-to-know basis.

4.52 The nature and frequency of the testing must be commensurate with:

a) the rate at which the vulnerabilities and threats change;

b) the criticality and sensitivity of the IT system or information asset;

c) the consequences of a security incident;

d) the risks associated with exposure to environments where a regulated institution is unable to enforce its security policies; and

e) the materiality and frequency of change to information assets.

4.53 Where a regulated institution's information assets are managed by third-party service providers, and the institution is reliant on that party's information security control testing, the institution must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with the guide outlined above.

4.54 All findings must be logged, assessed for severity, prioritised, and remediated promptly. Significant unresolved findings must be escalated to senior management and the Board for timely oversight and action.

4.55 Lessons learned from security testing and actual incidents should be used to continuously strengthen the institution's cyber resilience measures and response capabilities.

4.56 Where critical assets or services are outsourced, institutions shall ensure that third-party providers conduct testing that aligns with this guideline, including Red Team Testing for critical outsourced functions where appropriate.

4.57 Regulated institutions are required to participate in industry-wide threat intelligence sharing and coordinated sector-wide scenario-based exercises to strengthen collective cyber resilience.

4.58 All test plans, results, and remediation actions shall be documented, securely stored, and made available for regulatory review. All test data and reports must be protected under the institution's data protection policies and in compliance with all the legal requirements.

4.59 An institution should have processes and procedures in place to conduct ***post-incident analyses*** to identify root causes of its cybersecurity incidents and integrate its findings back into its response and recovery plans.

4.60 Where cyber incidents may affect the financial sector, regulated institutions should consult with relevant external stakeholders (regulators, cybersecurity agencies, other entities in the financial sector) to develop ***common response and recovery plans***.

Situational Awareness and Information Sharing

4.61 Strong situational awareness can significantly enhance a regulated institution's ability to understand and pre-empt cyber events, and to effectively detect, respond to and recover from cyber-attacks that are not prevented.

4.62 The institution should define the goals and objectives of information sharing, in line with its business objectives and cyber resilience framework.

4.63 At a minimum, the regulated institution should:

a) include in its objectives, collecting and exchanging information in a timely manner that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants during and following a cyber-attack;

b) define the scope of information-sharing activities by identifying the types of information available to be shared, including:

i) attackers' modus operandi, indicators of compromise, and threats and vulnerabilities, etc;

ii) the circumstances under which sharing this information is permitted (e.g. in the case of a cyber-incident);

iii) those with whom the information can and should be shared (e.g. the regulated institution's direct stakeholders such as critical service providers, participants and other interconnected regulated institutions, etc.); and

iv) how information provided to the regulated institution and other sector participants will be acted upon.

c) establish and regularly review the information-sharing rules and agreements and implement procedures that allow information to be shared promptly and in line with the objectives and scope established above, while at the same time meeting its obligations to protect potentially sensitive data that may have adverse consequences if disclosed improperly;

d) establish trusted and safe channels of communication with its direct stakeholders for exchanging information;

e) have in place a process to access and share information with external stakeholders in a timely manner, such as regulators, law enforcement or other institutions within the regulated institution's ecosystem;

f) participate actively in existing **information-sharing groups and facilities**, including cross-industry, cross-government and cross-border groups to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats;

g) establish and implement protocols for sharing information relating to threats, vulnerabilities and cyber incidents with employees, based on their specific roles and responsibilities;

h) incorporate lessons learned from its analysis of the cyber threat information into the employee training and awareness programs;

i) share information with relevant stakeholders in the ecosystem to achieve broader cyber resilience situational awareness, including promoting an understanding of each other's approach to achieving cyber resilience;

j) make use of threat intelligence capabilities that provide internal and external threat and vulnerability information, analyse this information, and disseminate it to the relevant stakeholders in the ecosystem promptly, so as to help stakeholders to respond quickly and mitigate risks; and

k) participate in efforts to identify the gaps in current information-sharing mechanisms and seek to address them, to facilitate a sector-wide response to large-scale incidents.

Cyber Exercises

4.64 A regulated institution should carry out regular ***scenario-based cyber exercises*** to validate its response and recovery, as well as ***communication plans*** against cyber threats.

4.65 Depending on the exercise objectives, regulated institutions should involve relevant stakeholders, including senior management, business functions, corporate communications, crisis management team, service providers, and technical staff responsible for cyber threat detection, response and recovery.

ICT Audit

4.66 Audit plays an important role to assess the effectiveness of cybersecurity controls, risk management and governance process in a regulated institution. Therefore, regulated institutions should ensure ICT audit is performed to provide the board of directors and senior management an independent and objective opinion of the adequacy and effectiveness of the regulated institution's risk management, governance and internal controls relative to its existing and emerging technology risks.

4.67 Regulated institutions should put in place a comprehensive set of auditable areas for technology risk so that an effective risk assessment could be performed during audit planning. Auditable areas should include all ICT operations, functions and processes.

4.68 ICT audits should be performed ***annually*** or more frequently commensurate with the risk posed by size and complexity of the ICT information asset, function or process.

4.69 A regulated institution should ensure its ICT auditors have the requisite level of competency and skills to effectively assess and evaluate the adequacy of ICT and cybersecurity policies, procedures, processes and controls implemented.

5. MANAGEMENT OF THIRD-PARTY SERVICE PROVIDERS

5.1 The financial sector is increasingly relying on third-party service providers of technology and other cloud services to support critical operations. While these arrangements can enhance efficiency and innovation, they also introduce significant cyber risks that must be proactively managed.

Governance and Oversight

5.2 The board of directors and senior management are ultimately responsible for ensuring that a robust governance framework is in place to identify, assess, monitor, and mitigate cyber risks associated with all third-party arrangements throughout the entire third-party lifecycle. This should be aligned with the institution's broader operational resilience framework taking into account interconnections and potential impact on critical operations.

Due Diligence and Risk Assessment

5.3 Before engaging any third-party, institutions must conduct comprehensive due diligence to identify and assess potential cyber risks. This should include:

a) Evaluating the provider's cybersecurity policies, controls, and resilience;

b) Understanding any subcontractors (fourth-party) dependencies;

c) Reviewing how the provider accesses, processes, stores, or transmits the institution's data; and

d) Obtaining independent security certifications and reports periodically.

5.4 Where an institution relies on **shared services or group-level service providers**, these arrangements must be subject to the same rigorous third-party cyber risk management processes as external third parties. This includes:

a) Full due diligence and risk assessment of intra-group shared services;

b) Regular monitoring of cyber resilience and security controls of group service providers;

c) Clear contractual or internal agreements outlining roles, responsibilities, and access rights; and

d) Effective information sharing of identified cyber risks and incidents across the regulated institution's group, particularly where the parent or service entity is foreign-owned, to ensure timely response and risk containment.

e) Where a regulated institution is part of a group, **group-wide cyber audits** for shared services and **cross-border data flow risk**

assessments should be conducted regularly. In addition, the group is required to formalise intra-group incident communication protocols.

Contractual Safeguards

5.5 Regulated institutions should ensure contracts with third parties capture cyber security considerations that are commensurate with the entity's cyber risk appetite.

5.6 Outsourcing arrangements must clearly define:

a) Cybersecurity roles and responsibilities for all parties;

b) Requirements for implementing and maintaining adequate security controls, including secure software development practices;

c) Rights to audit, monitor, and review the provider's security posture;

d) Provisions for data protection, data segregation (especially for cloud services), and data portability to prevent vendor lock-in; and

e) Business continuity, incident response, and exit arrangements.

Ongoing Monitoring and Review

5.7 Regulated institutions must regularly monitor and review third-party cyber risk through:

a) Periodic security assessments, including independent audits where necessary;

b) Continuous monitoring of connections and access, enforcing least privilege principles;

c) Maintaining an up-to-date inventory of third parties, group providers, and critical dependencies; and

d) Assessing substitutability of critical service providers and planning for alternative arrangements.

5.8 Institutions should conduct response and recovery testing with its third-party service providers and use the testing results to improve its response and recovery plans.

Supply Chain Risk Management

5.9 Regulated institutions must specifically assess supply chain risks linked to third parties supporting critical operations. This includes:

a) Understanding the full supply chain, including fourth-party dependencies;

b) Assessing end-to-end data processing and secure development practices; and

c) Conducting additional assurance reviews for high-risk software or service providers.

Threat Intelligence and Information Sharing

5.10 Institutions should expand cyber threat intelligence monitoring to cover key third parties, group providers, and technologies used. Identified threats should be shared within the institution and, where appropriate, with peer institutions to strengthen collective preparedness against supply chain and third-party attacks.

Preparedness and Incident Response

5.11 Institutions must integrate third-party and group service arrangements into incident response and business continuity plans. Scenario-based response strategies and regular drills should include critical third parties and shared services to test and refine response and recovery protocols.

Cloud Service Providers

5.12 Regulated entities should inform the Reserve Bank about their outsourcing of critical functions to cloud service providers early in their decision-making process.

5.13 In addition, where critical functions are outsourced to cloud service providers, institutions must:

a) Assess jurisdictional risks, compliance obligations, and data segregation requirements under the shared responsibility model;

b) Ensure the agreement includes explicit provisions for compliance with the data protection legislation covering storage, processing, and transmission of personal data; and

c) Reference international standards and industry best practices to validate the cloud provider's security posture.

Documentation and Reporting

5.14 An up-to-date, comprehensive inventory of all third-party and intra-group service providers, interconnections, and outsourced critical functions must be maintained. Institutions must demonstrate to the Reserve Bank that all related cyber risks are being effectively identified, managed, and reviewed on an ongoing basis.

6. CYBERSECURITY REQUIREMENTS FOR EMERGING TECHNOLOGIES

6.1 As the financial sector continues to modernise, institutions are increasingly adopting emerging technologies to enhance efficiency, customer experience, and innovation. While these technologies offer significant benefits, they introduce new and evolving cyber risks.

6.2 Regulated institutions must adopt proactive measures to secure their systems, data, and customers as they embrace these technological advancements.

6.3 The emerging technologies requiring adequate cybersecurity controls include:

a) Contactless and Mobile Payments (e.g. QR codes, Near Field Communication (NFC)

b) Voice-Activated Services

c) USSD-based Financial Services

d) Open Banking & API Integrations

e) Artificial Intelligence (AI) & Machine Learning (ML)

f) Cloud Computing

g) Distributed Ledger Technology (DLT)

h) Internet of Things (IoT)

i) Fintech-Connected Platforms

6.4 The following is a summary of key considerations and strategies for regulated institutions to ensure proactive data protection across platforms:

Risk Identification & Assessment

a) Regulated institutions should develop a strategy and risk-based framework for adopting emerging technologies.

b) Conduct a business case and cyber risk impact assessment before deployment.

c) Identify potential vulnerabilities, threat vectors, and data privacy concerns in alignment with local and international cybersecurity standards.

Core Security Control

a) Implement strong identity and access controls (e.g. Multifactor Authentication (MFA), role-based access).

b) Encrypt sensitive data in transit and at rest; adopt secure key management.

c) Conduct regular vulnerability assessments, penetration tests, and secure code reviews.

d) Apply secure API development practices: enforce access policies, monitor traffic, and throttle usage.

e) Establish layered security architecture to minimise risk from misconfigurations and third-party integrations.

f) Secure cloud deployments using industry benchmarks (e.g., CIS, NIST) and ensure data backups are encrypted and segregated.

g) Conduct due diligence and enforce strong Service Level Agreements (SLAs) with third-party providers.

h) Ensure data minimisation on edge/IoT devices and keep firmware updated.

i) Integrate business continuity and incident response plans to address emerging tech-specific disruptions.

Monitoring, Reporting & Compliance

a) Monitor the cybersecurity posture of adopted technologies and report periodically to executive management.

b) Maintain real-time threat detection, especially for AI- and IoT-enabled systems.

c) Track and address compliance with data privacy and cybersecurity regulations.

d) Ensure fintech and cloud providers operate within regulatory boundaries and maintain adequate cybersecurity standards.

e) Establish an incident response mechanism tailored to risks arising from emerging technologies.

Regulatory Compliance Requirements

a) Prior written approval from the Reserve Bank is required before implementing new technology platforms, launching digital financial services, or making significant changes to existing ICT infrastructure.

b) Institutions must also ensure that all third-party service providers are properly licensed and not subject to international sanctions or restrictions.

c) Institutions must maintain evidence of risk assessments, approvals, vendor due diligence, and technology audit trails for regulatory review.

7. CAPACITY BUILDING AND CONTINUOUS LEARNING

7.1 Regulated institutions should ensure that the board of directors, senior management, and all personnel have the necessary awareness, skills, and capacity to understand and manage cyber risks.

7.2 Cyber security training and awareness programs should be designed to equip an institution's employees with the knowledge and skills they need to protect the organisation's data and sensitive information from hacking, phishing, or other breaches which in turn will protect the IT infrastructure.

7.3 Regulated institutions should implement different aspects to cyber awareness training to give employees a holistic skillset for safely managing data and online activity.

7.4 The content of the training programme should at a minimum include information on the prevailing cyber threat landscape and its implications, the regulated institution's ICT security policies and standards, as well as an individual's responsibility to safeguard information assets.

7.5 All personnel in the institution should be made aware of the applicable laws, regulations, and guidelines pertaining to the use of, and access to, information assets.

7.6 The training programme should be conducted at least annually for all staff, contractors and service providers who have access to the institution's information assets.

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

7.8 The training programme should be reviewed periodically to ensure its contents remain current and relevant. The review should take into consideration changes in the regulated institution's ICT security policies, prevalent and emerging risks, and the evolving cyber threat landscape.

7.9 Each institution's program should be tailored based on capacity needs. At a minimum, the elements of cybersecurity threats and protection training should include the following:

- **Responsibility for the entity's data**: Employees should be aware of their responsibility for protecting sensitive information and complying with laws.
- **Password security**: Creating and using strong passwords, regular change of passwords.
- **Phishing awareness**: recognising potential phishing emails and avoiding scams or divulging privileged information.

- **Compliance** with regulations.
- **Data privacy**.
- **Insider threats** and vulnerabilities.
- **Procedures**: Understanding policies and protocols for responding to security incidents.
- **Appropriate online behavior and email use**.
- **Remote usage**: Protecting devices and systems while working remotely, such as by using VPNs or remote gateways.

7.10 Specialised technical training must be provided for IT and security personnel to ensure they remain current with evolving threats, tools, and defensive practices.

7.11 All training initiatives should be governed by a documented cybersecurity training programme, which is reviewed and updated regularly.

8. CYBER SECURITY COMMUNICATION AND INCIDENT REPORTING

8.1 Effective communication in cyber security enables regulated institutions to stay informed about the latest threats and vulnerabilities, share information and best practices, which enables them to respond more effectively to emerging threats.

8.2 Timely and effective communication is essential to contain the damage and prevent further breaches when a cyber attach occurs. Communication enables an institution to coordinate response efforts, share information with stakeholders, and provide updates to affected parties.

8.3 In addition, in the event of a cyber attack, transparency and communication are essential to maintain stakeholder trust and confidence. Organisations that communicate effectively and transparently are more likely to maintain the trust of their customers, partners, and investors.

Communication Channels

8.4 Regulated institutions should plan for information sharing through trusted channels: collecting and exchanging timely information that could facilitate the detection, response and recovery of systems from cyber incidents.

8.5 The entity should meet relevant regulatory requirements for reporting information regarding cyber incidents and cyber resilience preparedness.

8.6 An institution's communication strategy should include the following types of communication in cyber security:

a) **Internal Communication** within the organisation, including communication between employees, teams, and departments;

b) **External Communication** with external stakeholders, including customers, partners, and vendors;

c) **Information Sharing** with other institutions and industry groups; and

d) **Incident Response Communication** during a cyber attack or incident, including communication with stakeholders and affected parties.

8.7 Regulated entities should also determine beforehand which types of information will be shared, the circumstances under which sharing is permitted, with whom the information can and should be shared, and how the information provided to the entity should be acted upon.

8.8 The process of information sharing, especially contact information, should be maintained and updated regularly.

Regulatory Reporting

8.9 Regulated institutions should maintain proactive and transparent communication which is aligned with regulatory expectations to support sector-wide cyber resilience.

8.10 Regulated institutions must conduct **annual cybersecurity self-assessments** as of 31 December each year and submit results to the Reserve Bank by 15 February. The institutions should refer to the baseline guide in **Appendix 4** which provides a checklist to guide self-assessments.

8.11 Institutions should report all confirmed cybersecurity incidents to the Reserve Bank **within three hours of detection**, or as soon as the institution becomes aware of the incident. Reports must follow the format outlined in **Appendix 3**, which incorporates **initial incident reports**, **update incident reports** and **concluding incident reports**

8.12 Institutions must also submit quarterly incident reports capturing all actual or attempted cyber-attacks. These submissions must adhere to the format and timelines prescribed by the Reserve Bank.

8.13 This regular communication is critical for coordinating sector-wide response to cyber threats and for supporting national cybersecurity situational awareness and preparedness.

ENQUIRIES

Any enquiries relating to this Guideline should be addressed to **Reserve Bank of Zimbabwe, 80 Samora Machel Avenue, Harare** to the attention of

- Director
  Bank Supervision, Surveillance and Financial Stability

and/or

- Deputy Director
  National Payment Systems

9. APPENDICES

Appendix 1: Definitions of Terms

Unless otherwise specified, terms used and defined in the Banking Act [Chapter 24:20] ("the Banking Act) or the Microfinance Act [Chapter 24:30] ("the Microfinance Act") or the National Payment Systems Act [Chapter 24:23] ("NPS Act") shall have the meanings ascribed in the said laws. In addition, for the purposes of this Guideline, the following definition of terms and acronyms apply:

Business Continuity (BC) is a state of continued and uninterrupted operation of a business.

Business Continuity Plan (BCP) is a comprehensive, documented plan of action that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an institution in the event of a disruption.

CISO is an acronym referring to the chief information security officer. He/ She is the senior-level executive within an organisation responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

Cyber-crime or the cyber threat refers to a harmful activity, executed by one group or individual through computers, Information and Communication Technology (ICT) systems and/or the internet and targeting the computers, ICT infrastructure and internet presence of another entity (According to the International Organisation of Securities Commissions (IOSCO).

Cyber environment refers to users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to the network.

Cyber resilience refers to the regulated institution's ability to prepare for, respond to, recover from cyberattacks and data breaches while continuing to operate with no or minimal instability.

Cyber risk is any risk arising from a failure of an institution's information technology systems resulting in financial loss, disruption of services, and interference with business as usual or damage to the reputation of an institution.

Cybersecurity is an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation.

Cybersecurity incident is any malicious act or suspicious event that: compromises, or attempts to compromise, the electronic security perimeter or physical security

perimeter of a critical Cyber Asset or disrupts or attempts to disrupt, the operation of a critical Cyber Asset.

Cybersecurity standards are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organisation.

Black box testing is a software testing technique in which the tester doesn't know the internal structure, design and implementation of the software application that is being tested.

Gray box testing is a software testing technique which is a combination of black box testing technique and white box testing technique. The internal structure, design and implementation is partially known in Gray Box Testing.

White Box Testing is a software testing method in which the internal structure/ design/ implementation of the item being tested is known to the tester.

Ecosystem is a system or group of interconnected elements, formed linkages and dependencies. For a financial institution, this may include participants, linked financial institutions, service providers, vendors and vendor products.

Outsourcing means the contracting or sub-contracting of one or more activities relating to the operation of a system or the issuance and management of a payment instrument to an independent third party. Such third party provides services to the issuer.

Penetration testing is a test methodology in which assessors, using all available documentation (for example, system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

Recover - To restore any capabilities or services that have been impaired due to a cyber event.

Recovery Point Objective (RPO) is a key metric used in disaster recovery and business continuity planning to define the maximum acceptable amount of data loss measured in time. In other words, it represents the point in time to which data must be restored after a disruption or disaster.

Recovery Time Objective (RTO) is a key metric in disaster recovery and business continuity planning that defines the maximum acceptable amount of time within which a system, application, or process must be restored after a disruption or disaster. Essentially, RTO represents the target time frame for restoring business operations and systems to normal functionality following an incident.

Risk-based Cyber Risk Management is an approach whereby regulated institutions identify, assess and understand the risks to which they are exposed to and take effective measures commensurate with these risks.

Security Operation Centre (SOC) is a centralised function within an organisation employing people, processes, and technology to continuously monitor and improve an organisation's security posture while preventing, detecting, analysing, and responding to cybersecurity incidents.

Situational awareness is 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 in mitigating the impact of a potentially harmful event.

Tactics, techniques and procedures (TTPs) explain the behaviour of a threat actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

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

Threat-led penetration testing (TLPT) (also known as red team testing) is a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques, and procedures of real-life threat actors. It is based on targeted threat intelligence and focusses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations.

Vulnerability is a weakness, susceptibility, or flaw of an asset or control that can be exploited by one or more threats.

Vulnerability assessment is 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.

Appendix 2: Acronyms

AI - Artificial intelligence

AIM - Asset Inventory Management

BCP – Business Continuity Plan

CBEST - Critical National Infrastructure Banking Supervision and Evaluation Testing

CIS - Centre for Internet Security

CISO – Chief Information Security Officer

DDoS - Distributed Denial of Service

DLT - Distributed Ledger Technology

DMZ - Demilitarised Zone

ICT – Information and Communication Technologies

IDS – Intrusion Detection System

IOSCO - International Organisation of Securities Commissions

IoT - Internet of Things

ICT – Information and Communication Technologies

MFA - Multifactor Authentication

ML – Machine Learning

IP - Internet Protocol

IPS - Intrusion Prevention System,

ISO - International Organisation for Standardisation

ISAC - Information Sharing and Analysis Centres

ISMS - Information Security Management System

NFC - Near Field Communication

NIST - National Institute of Standards and Technology

NPS - National Payment Systems

TIBER-EU - Threat Intelligence-based Ethical Red Teaming - European Union

TTPs - tactics, techniques and procedures

RPO - Recovery Point Objective

RTO - Recovery Time Objective

SADC-PSOC - Southern African Development Community Payment Systems Oversight Committee

SDLC - System Development Life Cycle

SIEM - Security Information and Event Management

SOC - Security Operation Centre

VPN - Virtual Private Network

Appendix 3: Cyber Resilience Reporting Templates

BSD 7 - Cyber Incident Notification Report.xlsx

BSD 8 - Periodic Cyber Incident Report.xlsx

Appendix 4: Baseline Cyber Security and Resilience Requirements

1. This section sets out cybersecurity and resilience requirements for regulated institutions to achieve baseline cyber-security/resilience.
2. Institutions are expected to review and update their cybersecurity posture regularly to address evolving threats, emerging technologies, and changes in business models or digital service offerings.
3. This baseline may be evaluated periodically to integrate risks that arise due to new threats, products or processes. Some of the key points to be kept in mind are:
    a. Given the increasing adoption of digital technologies and associated risks, institutions should regularly assess the structure and effectiveness of their IT and cybersecurity functions. Active oversight at the board level is essential to set a strong governance tone.
    b. Institutions must maintain a proactive posture, anticipating threats rather than reacting to them.
    c. Cybersecurity teams should be equipped to monitor system logs and security incidents in real-time or near real-time, supported by appropriate tools and staffing.
    d. Continuous vigilance is critical and institutions must remain alert to new attack vectors and evolving tactics.
    e. Security tools and infrastructure must be correctly configured and regularly reviewed to ensure they are effective.
    f. People are the first line of defense. Regular training, clear communication of the institution's security policies, and ongoing awareness programs are essential to building a resilient cyber culture.

Governance & Strategy

4. The board of directors must oversee cybersecurity governance by ensuring appropriate structures are in place, including the appointment of a Chief Information Security Officer (CISO) or equivalent.
5. In smaller institutions, the CISO role may be integrated within the broader risk management function.
6. Cybersecurity responsibilities must be clearly defined across the organisation.
7. Each institution is required to establish a documented cyber resilience strategy that addresses governance, risk identification, protection, detection, and response and recovery mechanisms.

8. This framework must be updated annually, with interim revisions carried out when significant operational or technological changes occur.
9. Cyber risks should be formally reviewed at least once every quarter.
10. Institutions should conduct background checks on personnel with privileged system access. The frequency and depth of such checks should be proportionate to the sensitivity of the role, e.g. every year for users with access to high-risk platforms.
11. Regulated institutions should set aside board approved risk-based budgets specifically for Cyber Security Management.

Asset and Inventory Management

12. All regulated institutions must maintain a comprehensive, accurate, and continuously updated inventory of all IT assets. This includes hardware, software, personnel, data, and third-party services.
13. Each asset should be clearly classified according to business criticality, based on criteria defined by the institution.
14. Institutions are recommended to use automated tools to manage their asset inventory and detect unauthorised devices or applications.
15. A centralised and regularly maintained inventory of both authorised and unauthorised software must be in place.
16. Mechanisms must be established to control software installation on all devices and to prevent the execution of unauthorised applications.
17. The institution must maintain an up-to-date network architecture diagram that identifies all critical systems, security infrastructure, and external connections.
18. All network devices, including wireless components, must be securely configured and periodically reviewed to ensure compliance with established security baselines.
19. Access to the network should be actively controlled and monitored based on device compliance, with systems in place to detect unauthorised devices or suspicious activity.
20. Standard operating procedures must be developed and enforced for all major IT functions, including the onboarding of new devices or systems.
21. Institutions must maintain strict physical security measures to protect critical infrastructure and ensure that critical assets are housed in secure environments with protection against environmental and physical threats.
22. Environmental controls must be implemented to monitor and alert on anomalies such as excessive temperature, humidity, smoke, water ingress, power outages,

or communication failures. Breaches of these controls must trigger timely alerts and responses.

23. A formal exception management framework must be in place, defining the approval process, duration, review mechanisms, and authority for managing deviations from standard policies.
24. Changes to infrastructure must be tested in a User Acceptance Testing (UAT) environment that closely mirrors the production environment.
25. Regular penetration testing must also be conducted to identify and remediate vulnerabilities in critical systems.

Secure Configuration and Application Security

26. Regulated institutions must establish and maintain documented baseline security configurations for all systems and devices. These configurations should be regularly reviewed and updated.
27. Critical devices, including those hosted by third parties, must be evaluated and patched in a timely manner.
28. Security must be embedded throughout the entire application development life cycle.
29. Institutions must enforce secure coding practices, conduct source code reviews, and maintain strict segregation between development, testing, and production environments.
30. Security requirements such as access controls and logging must be defined early in the development process, with secure rollout strategies addressing known vulnerabilities.
31. Any new technologies must undergo risk assessments before deployment.

Patch, Vulnerability, and Change Management

32. A risk-based patching strategy must be in place, with all patches tracked to ensure timely implementation.
33. Institutions must regularly conduct vulnerability scans and penetration testing to identify and address security gaps.
34. All network access points should be secured, and identified vulnerabilities remediated as part of an integrated change management process.

Access and Identity Management

35. Regulated institutions should implement appropriate access control measures proportional to their operational needs and risk profile, selecting suitable models (e.g. role-based, attribute-based, or hybrid approaches) based on their organisational structure, technical capabilities, and regulatory requirements, while applying stronger authentication for sensitive functions like privileged access, remote connectivity, and high-risk transactions, with provisions for regular reviews to ensure continued effectiveness against evolving threats.
36. Regulated institutions should implement appropriate safeguards to protect sensitive data, both during transmission and while stored.
37. Measures should include encryption and secure communication methods aligned with the institution's risk profile and the sensitivity of the data.
38. Dormant accounts must be promptly deactivated, and login anomalies should be monitored.
39. Device compliance must be enforced, and unauthorised software installations and access attempts should be blocked.

Customer Authentication and Secure Communication

40. Institutions must implement robust authentication frameworks to verify their identity to customers and ensure secure access for third-party systems.
41. Email and messaging platforms should be secured against spoofing, malware, and unauthorised access through appropriate configuration and control mechanisms.

Data Protection and Privacy

42. Sensitive data must be encrypted both in transit and at rest using industry standards.
43. Institutions must maintain comprehensive data loss prevention (DLP) strategies, which are reviewed periodically and at least annually and extended to vendor-managed environments.
44. A defined policy must be in place to restrict and securely manage the use of removable media, with all devices scanned for malware.
45. Similar arrangements need to be ensured at the vendor managed facilities as well.

Threat Defense and Monitoring

46. Institutions must implement centralised anti-malware and antivirus systems, with consideration given to web whitelisting and secure gateways.
47. Audit logs must be systematically collected, analysed, and retained to detect and respond to suspicious activities.
48. Settings for audit trails must be periodically validated to ensure completeness and accuracy.
49. Log collection scope, frequency, and retention should be determined in consultation with relevant stakeholders.

Advanced Threat Detection and Red Teaming

50. Institutions must perform regular vulnerability assessments, penetration testing, and red team exercises on critical systems.
51. All identified vulnerabilities must be remediated in line with the institution's risk management policies and timelines.

Incident Response and Business Continuity

52. An institution-wide incident response plan must be in place, with clearly defined roles, board approval, and provisions for continual improvement.
53. Cyber resilience should be fully integrated into the broader business continuity and disaster recovery plans, ensuring rapid recovery and minimal downtime during a cyber event.
54. Cybersecurity incidents must be reported to the Reserve Bank within 3 hours.

Fraud and Transaction Monitoring

55. Institutions must implement risk-based transaction monitoring across all service delivery channels.
56. Customers should be notified via alternative communication channels for transactions exceeding predefined thresholds to enhance fraud prevention.

Metrics and Forensics

57. Key performance and risk indicators including incident trends, vulnerabilities, and compliance gaps should be tracked and reviewed regularly.

58. Institutions must establish a dedicated team to support forensic investigations and respond effectively to cyber incidents.

User, Employee, and Management Awareness

59. Security policies must be clearly defined and communicated to all internal stakeholders, covering responsible use of systems and data.
60. Regular cybersecurity training must be provided to staff, with specialised sessions for senior management and board members.
61. Specialised technical training must be provided for IT and security personnel to ensure they remain current with evolving threats, tools, and defensive practices.
62. All training initiatives should be governed by a documented cybersecurity training programme, which is reviewed and updated regularly.
63. A dedicated budget must be allocated to support the implementation and continuous improvement of the institution's cybersecurity awareness and training strategy.
64. Institutions should also foster a security-first culture by encouraging staff to report suspicious activity without fear of reprisal and ensuring that such reports are promptly assessed and acted upon.

Customer Education and Protection

65. Customers must be educated about cybersecurity threats such as phishing and social engineering.
66. Institutions should encourage prompt reporting of suspicious messages and ensure responsive action is taken.
67. Customers must also be informed about the risks of sharing credentials and the implications of doing so.

Third-Party and Vendor Risk Management

68. Institutions are fully accountable for the cybersecurity of outsourced services.
69. Comprehensive due diligence must be conducted before vendor onboarding, and vendor security controls must be evaluated regularly.
70. Contracts must include audit rights, data protection clauses, and exit strategies.

Information Sharing and Collaboration

71. Institutions should share cybersecurity threat intelligence with one another, especially during active attacks, to improve collective defense and institutional preparedness.

72. In addition to real-time collaboration, institutions must submit quarterly reports to the Reserve Bank detailing actual or attempted cybersecurity incidents. These reports must be submitted in a format and manner as may be prescribed by the Reserve Bank, enabling ongoing supervisory oversight and sector-wide risk analysis.

Maintenance, Monitoring and Analysis of Audit Logs

73. Institutions must implement and regularly validate audit log settings to ensure that all critical systems generate appropriate and complete audit trails, capturing essential information such as user activity, access events, and system changes.

74. Before determining the scope, frequency, and retention period of log collection, all relevant stakeholders should be consulted to ensure alignment with operational, compliance, and security needs.

75. Collected logs must be systematically managed and analysed to support the timely detection, investigation, and response to potential cybersecurity incidents.

10. REFERENCES

- Bank for International Settlements (BIS) and International Organisation of Securities Commissions (IOSCO). (2016). Guidance on cyber resilience for financial market infrastructures, SBN 978-92-9197-288-3. https://www.bis.org/cpmi/publ/d146.pdf.
- Bank for International Settlements (BIS). (2018). Cyber-resilience: Range of Practices. Basel. https://www.bis.org/bcbs/publ/d454.pdf.
- CREST (2023). Fostering Financial Sector Cyber Resilience in Developing Countries. The Way Towards Threat Penetration Testing, https://cmage.crest-approved.org/fostering-cyber-resilience.pdf
- Cyber and Data Protection Act, 2021 [*Chapter 12:07]*
- Deloitte (2020) report on "New considerations for governing cloud services for financial institutions" https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-new-considerations-for-governing-cloud-services-for-financial-institutions.pdf
- European Banking Authority (EBA). (2017). Final draft Recommendations on Cloud Outsourcing. EBA/REC/2017/03.
- European Union Data Protection Code of Conduct for Cloud Service Providers. https://eucoc.cloud/fileadmin/cloud-coc/files/former-versions/European_Cloud_Code_of_Conduct_1-7.pdf
- Financial Stability Board (FSB). (2020). "Effective Practices for Cyber Incident Response and Recovery: Consultative Document." Basel. https://www.fsb.org/wp-content/uploads/P200420-1.pdf.Monetary Authority of Singapore, Technology Risk Management Guidelines.
- General Data Protection Regulation (GDPR). (2018)
- Global Financial Markets Association (GFMA). (2020). A Framework for Threat-Led Penetration Testing in the Financial Services Industry by the https://www.gfma.org/wp-content/uploads/2020/12/gfma-penetration-testing-guidance-for-regulators-and-financial-firms-version-2-december-2020.pdf
- Hart, D. V. (2019). Factors Influencing the Adoption of Cybersecurity Situational Awareness Programs. ISACA Journal, 5. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-5/factors-influencing-the-adoption-of-cybersecurity-situational-awareness-programs_joa_eng_0919.pdf
- International Monetary fund (IMF). (2020). Staff Discussion Note, Cyber Risk and Financial Stability: It's a Small World After All.
- Jai Sisodia and Mohammed Khan. (2022). Understanding the Shared Responsibilities Model in Cloud Services. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/understanding-the-shared-responsibilities-model-in-cloud-services

- KPMG. (2017). Top 10 Internal Audit Focus Areas for Technology companies. https://assets.kpmg.com/content/dam/kpmg/is/pdf/2018/07/kpmg-top-10-internal-audit-tech-2017.pdf
- McKinsey & Company. (2022) Risk & Resilience Practice Cybersecurity trends: Looking over the horizon.
- National Institute of Standards and Technology. (2011). Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-1444 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-144.pdf
- National Institute of Standards and Technology (NIST). (2021). Special Publication 800-160, Volume 2 Revision 1, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,"

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
- Office of the Comptroller of the Currency (OCC). (2024). Third-Party Risk Management A Guide for Community Banks. https://www.occ.gov/news-issuances/news-releases/2024/pub-third-party-risk-management-guide-for-community-banks.pdf
- The Association of Banks in Singapore (ABS). (2015) Penetration Testing Guidelines for the Financial Industry in Singapore https://www.abs.org.sg/docs/library/abs-pen-test-guidelines.pdf?sfvrsn=b284c86f_0
- Reserve Bank of New Zealand. https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/consultations/cyber-resilience/guidance-on-cyber-resilience.pdf
- World Bank (WB). 2019. "Cyber Resilience for Financial Market Infrastructures." Washington, DC. http://pubdocs.worldbank.org/en/189821576699037673/FIGI-ECB-OperationalCyberFinalWeb-12-13.pdf.