# Contents

1. APPLICABILITY .................................................................................................................................. 3  
2. POLICY STATEMENT .......................................................................................................................... 3  
3. DEFINITIONS ..................................................................................................................................... 6  
4. INTRODUCTION ................................................................................................................................... 9  
5. MINIMUM CONTENTS OF A CYBERSECURITY POLICY ................................................................... 11  
6. GOVERNANCE AND BOARD OVERSIGHT ..................................................................................... 13  
7. CYBERSECURITY RISK MANAGEMENT SYSTEM ............................................................................. 20  
8. ROLE OF RISK MANAGEMENT FUNCTION ...................................................................................... 22  
9. DIGITAL FINANCIAL SERVICES ........................................................................................................ 23  
10. TRAINING/AWARENESS .................................................................................................................... 24  
11. SUBMISSIONS OF REPORTS ............................................................................................................... 25
1 APPLICABILITY

1.1 Authorisation

1.1.1 The Risk Based Cyber Security Guideline is issued pursuant to the National Payment Systems (NPS) Act (Chapter 24:23).

1.2 Application

1.2.1 This Guideline applies to all institutions licensed under the National Payment Systems, Banking and any related Acts under the Reserve Bank of Zimbabwe’s jurisdiction.

2 POLICY STATEMENT

2.1 Policy Thrust

2.1.1 The Bank continues with its mandate to ensure financial stability in the market and creating an enabling environment for existing and new initiatives which are also meant to enhance the public interest objectives in an inclusive manner.

2.1.2 However, due to the highly digitalised economy in the context of the Fourth Industrial Revolution, cyber risks are increasingly targeting and leveraging on financial market infrastructures. The international community through various bodies have heightened their awareness and prescribe some workable measures.

2.1.3 The Zimbabwean financial services community has embraced some measures from organisations such as the Bank for International Settlement (BIS). While the principles and expectations of this cybersecurity guideline incorporates risk management areas that are outlined in the 24 Principles for Financial Market Infrastructures (PFMIs), the Guideline is not intended to replace or supersede the international best practices.

2.1.4 In the case where the institutions cybersecurity operations depart from the BIS cyber security guideline, they shall identify and demonstrate to the Bank, any identified international best practise guidelines they would have put in place.

2.2 Background

2.2.1 The world of cybersecurity is ever-changing and cyber-attacks continue to expand in scale and scope. It’s nearly impossible to single-handedly keep up with the evolving threat to cybersecurity best practices, especially when many information technology teams need to balance with competing priorities given the limited resources availed to them.

2.2.2 Zimbabwe, as part of the global village and has over the years progressively adopted and modestly migrated to largely digital economy in particular the financial services sector. This is clearly backed by the Reserve Bank’s policy thrust towards the use of digital financial services and its success is attributable to collaborative efforts, commitment, action and market innovation which have continued to drive the digital economy revolution.

2.2.3 However, evidence at hand has shown a growing trend in cyber risk threats in the financial services sector. Notably, the increasing sophistication, frequency and persistence of cyber risks remains growing concern of the authorities and key stakeholders as it threatens to reverse the positive achievements to date.

2.2.4 This Guideline therefore outlines the minimum requirements that institutions shall build upon in the development and implementation of strategies, policies, procedures and related activities aimed at mitigating cyber risk in developing digital economy.


2.3 Purpose

2.3.1 The purpose of this Guideline is to provide key guiding principles and best practices that will offer guidance to assist regulated entities and authorities in devising tools for the financial sector to deal with cyber security risks as outlined in this document.

2.3.2 Assist financial market infrastructures (FMIIs), payment services providers (PSPs) and participant banks (which are hereinafter referred to as financial institutions) strengthen their cyber-risk management in the provision of services;

2.3.2.1 Create a secure cyber ecosystem in the financial services sector through generation of adequate trust and confidence in the digital market infrastructures during the processing of financial services or transactions;

2.3.2.2 Create a safer and more secure cyberspace that underpins information system security priorities and promote stability of the financial services sector;

2.3.2.3 Establish a coordinated approach to the prevention and combating of cybercrime;

2.3.2.4 Up-scale identification and protection of critical information infrastructure;

2.3.2.5 Promote compliance with appropriate technical and operational cybersecurity standards;

2.3.2.6 Develop requisite skills, continuous capacity building, public awareness, and promote a culture of fostering a strong interplay between policy, leveraging on technology to do business and risk management;

2.3.2.7 Continue to implement cybersecurity measures that enhance upholding and maintaining of public trust in the financial services sector; and,

2.3.2.8 Promoting coordination, information sharing, cooperation and collaboration of local, regional and global stakeholders on cyber security.
2.4 Scope and Coverage

2.4.1 This Guideline sets the minimum standards that FMIs, PSPs and participating banks should adopt to develop effective cybersecurity governance and risk management frameworks.

2.4.2 It does not supersede the existing legislation, regulations and guidelines that institutions must comply with as part of their regulatory obligations with particular reference to risk management, outsourcing, information communication technology, internal controls and corporate governance.

2.5 Responsibility

2.5.1 The Reserve Bank will review the financial institutions’ policies on an ongoing basis to assess their appropriateness in line with the practices contained in the Bank of International Settlement (BIS) cyber resilience guidance principles.

2.5.2 In the event that results of the assessment are unsatisfactory, the Bank may require the institution involved to enhance the risk management policies, processes or procedures, or to hold additional capital.

2.5.3 However, where there are material differences between the guideline and the cyber resilience practice in place, the institution should provide reasons for such.

2.6 Obligations of Regulated Entities

2.6.1 Reserve Bank regulated institutions shall perform the following obligations:

2.6.1.1 Place special emphasis on cyber and information security and take all the necessary steps to protect and manage their systems and data effectively.

2.6.1.2 Expand and enhance their cyber and information security capabilities.

2.6.1.3 Improve the institution’s resilience to operational disruptions due to the materialisation of cyber and information security risks; reduce their impact on the institution’s business continuity, and to minimise damage to its ICT assets and information including those of its customers.

2.6.1.4 Manage cyber and information security risks with a systemic, organization-wide view, within the framework of the Zimbabwean law and subject to its Policy Management Framework pertaining to the cyber risk universe, and ICT management.

2.6.1.5 Document the cyber and information risks relevant to its operations as well as the measures taken to mitigate them.

2.6.1.6 Address cyber and information security scenarios that may affect its own activities and those of customers, suppliers and service providers.

2.6.1.7 Share cyber information security attacks which relate to the institution’s activities or business with the regulators and other institutions, these should include those of customers, suppliers as well as service providers.

2.6.1.8 Understand the scope of cyber and information security threat and the required security capabilities for meeting this challenge.

2.6.1.9 Strive to be compliant with recognised international and regional security standards including SADC payment systems standards among others.

2.6.1.10 Institutions that handle, process, store, or transmit debit card, credit card, prepaid card, e-money and related information shall be certified by recognised bodies in the respective sectors.
3 DEFINITIONS

The terms and acronyms used in this Guideline are defined below:

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

ii) ‘Business Continuity Management’ (BCM) is a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations can be maintained or recovered in a timely manner in the event of disruption. Its purpose is to minimise the operations, financial, legal, reputational and other material consequences arising from disruption.

iii) 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 organisation in the event of a disruption.

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

v) ‘Cyber-crime’ According to the International Organization of Securities Commissions (IOSCO), ‘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.

vi) Cyber environment: 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.

vii) ‘Cyber resilience’ refers to the financial institution’s ability to prepare for, respond to, recover from cyberattacks and data breaches while continuing to operate with no or minimal instability.

viii) Cyber resilience is the ability of an FMI to: (i) maintain essential operational capabilities under adverse conditions or stress, even if in a degraded or debilitated state; and (ii) recover to effective operational capability in a time frame consistent with the provision of critical economic services

ix) ‘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.

x) ‘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, unauthorized use or modification, or exploitation.

xi) ‘Cyberspace’ is the virtual space created by interconnected computers and computer networks on the internet.
‘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 organization.

Digital Financial Channels refer to the internet, computer based, mobile phones, large value platforms (RTGS/CSD systems), access points and devices (ATMs, POS terminals) among others authorised to operate by the Reserve Bank of Zimbabwe.

Digital Financial Services (DFS) include a broad range of financial services accessed and delivered through electronic channels, including payments, mobile money, credit, savings, remittances and insurance among others. DFS concept includes intra and inter entity transactional activities (MFS).

‘Ecosystem’ is a system or group of interconnected elements, formed linkages and dependencies. For an FMI, this may include participants, linked FMIs, service providers, vendors and vendor products.

Financial Market Infrastructure (FMI) refers to a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions.

Financial Institution refers -
(a) a banking institution registered in terms of the Banking Act [Chapter 24:20]; or
(b) any other institution which lawfully engages in the banking and payment system activities specified in paragraphs (a), (d) and (f) of subsection (1) of section seven of the Banking Act [Chapter 24:20] and National Payment Systems (NPS) Act [Chapter. 24:23];

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.

Payment Service Provider (PSP) means an entity that provides services enabling funds to be deposited and withdrawn from an account; payment transactions involving transfers of funds; the issuance and/or acquisition of payment instruments such as cheques, money, credit cards, debit cards; remittances and other services central to the transfer of funds. Also used interchangeably with FMI.

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

Risk-based Cyber Risk Management is an approach whereby financial institutions identify, assess and understand the risks to which they are exposed to and take effective measures commensurate with these risks.
Risk-based Cyber Risk Management is an approach whereby financial institutions identify, assess and understand the risks to which they are exposed to and take effective measures commensurate with these risks.
4.1 The ever-increasing surge in technology gives rise to cybersecurity risks and it is unavoidable as criminals exploit the digital financial ecosystems.

4.2 Cyber risks are one of the top ten (10) global risks of highest concern for the next decade, according to the World Economic Forum Global Risks Report 2019, with data fraud and theft ranked fourth and cyberattacks fifth among these.

4.3 Notably, the global outbreak of the Coronavirus (“COVID19”) has indisputably led to a paradigm shift in the way in which digital financial services is operating both internationally and locally.

4.4 Furthermore, Cybercrime is a major component of the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) concerns. It is on the list of twenty-one prescribed predicate offences as listed by the Financial Action Task Force (FATF).

4.5 The National Risk Assessment (NRA) Report, of 2020, cites cyber risks particularly through digital financial channels among other crimes as contributing currently an estimated US 900 million of illicit proceeds generated from criminal activity annually in Zimbabwe.

4.6 Consistent with that, the Central Bank continuous efforts in combatting online financial criminal activity dovetails and compliments the Government’s National ICT Policy and the National Cyber Security Policy intended to secure the Zimbabwean cyberspace against cyber-attacks.

4.7 Therefore, the need for cyber resilience and securing of end to end points in the ecosystem of the financial services cannot be over emphasised. Endpoints can range from the more commonly thought of devices like laptops, mobile devices, printers, servers and payment systems devices.

4.8 If a device is connected to a network, it is considered an endpoint. With the growing popularity of BYOD (bring your own device) and IoT (internet of things), the number of devices connected to an organization's network can quickly reach into the tens (and hundreds) of thousands.
The Table below provides some illustrations of cybercrime activities across the globe:

**Table: Examples of cybercrime activities**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interconnectedness of institutions could lead to compromise in the institutions entry points such as through service providers.</td>
</tr>
<tr>
<td>Improper access to privileged accounts – A non-privileged user who gains access to a privileged account could control the entire system. For example, hiding criminal acts by modifying or deleting log files or disabling detection mechanisms.</td>
</tr>
<tr>
<td>People related attacks like phishing, malware introductions through social engineering that can be utilized to gain privileged system access to critical systems.</td>
</tr>
<tr>
<td>Noncompliance with institutions’ databases exposing data to cyber criminals.</td>
</tr>
<tr>
<td>Internal ICT systems can themselves be a source of cyber risk. For example, data replication arrangements that are meant to safeguard business continuity could transfer malware or corrupted data to the backup systems.</td>
</tr>
<tr>
<td>Poor authentication controls to protect customer data, transactions and systems.</td>
</tr>
</tbody>
</table>

### 5 Minimum Contents of a Cybersecurity Policy

Financial institutions should utilise their existing governance structures to establish, oversee, formulate and implement an effective cyber security resilience policy that enables them to identify, protect, respond, detect, adapt and recover timeously without compromising stability of the ecosystem.

#### 5.1 Cyber Resilience

5.1.1 According to the BIS, cyber resilience ensures that business operations are safeguarded and a threat or breach should not demobilize the entire business activities but promote financial stability based on continuity with minimal or no disruptions.

5.1.2 Cyber resilience is a node on the cyber-security continuum, it represents a shift in paradigm from the conventional approach that seeks to prevent cyber-attacks to a more agile and adaptive stance.

5.1.3 Largely guided by principle of agility, cyber resilience goes beyond BCP and DR approach.

5.1.4 Simplified, cyber resilience is the ability of an organization to perceive, resist and react to disruptive events while adjusting, adapting and evolving where necessary.

#### 5.2 The Cybersecurity Policy

At a minimum the cyber security policy should generally contain the following:

5.2.1 **Governance and Oversight:** Mechanisms put in place to establish, implement and review the approach to managing cyber risks.

5.2.2 **Identification:** Operational failure can negatively impact financial stability hence the PSPs and financial institutions are required to identify their critical business functions and supporting information assets so as to safeguard them against compromise. An institution should identify its business functions and supporting processes and conduct a risk assessment in order to ensure that it thoroughly understands the importance of each function and supporting processes, and their interdependencies, in performing its functions. Identified business functions and processes should then be classified in terms of criticality, which in turn should guide the institution’s prioritisation of its protective, detective, response and recovery efforts.
5.2.3 **Protection:** Cyber resilience depends on effective security controls that protect the confidentiality, integrity and availability of assets and services. Physical and logical access to systems should be permitted only for individuals who are authorised, and authorisation should be limited to individuals who are appropriately trained and monitored. Protect all systems against malware and regularly update anti-viruses’ software or programmes as well as incorporate network segregation where appropriate.

It is mandatory for institutions to comply with the following requirements:

i. Establish, secure the environment and implement a robust security for ICT systems;
ii. Ensure updates are applied to address system security flaws in a timely manner;
iii. Deploy security devices to restrict unauthorised network traffic and physical access to key systems;
iv. Implement measures to mitigate the risk of malware infection;
v. Secure, know and limit access to the use of system accounts with special privileges to prevent unauthorised access; and
vi. Strengthen user authentication for critical systems as well as systems used to access customer information.

5.2.4 **Detection:** Financial institution’s ability to detect the occurrence of anomalies and events indicating a potential cyber incident is essential to strong cyber resilience. Early detection provides a financial institution with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches.

5.2.5 **Share cyber and information security attacks** with regulator and counterparties that affected the institution’s own activities and those of customers, suppliers and service providers;

5.2.6 **Resumption:** This relates to response and recovery and provides guidance on how a financial institution should respond in order to contain, resume and recover from successful cyber-attacks.
5.2.7 **Testing:** Once employed within a financial institution, the elements of its cyber resilience framework should be rigorously tested to determine their overall effectiveness.

5.2.8 **Situational awareness:** Strong situational awareness can significantly enhance a financial 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.

5.2.9 **Learning and evolving:** Financial institutions should aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the institution.

5.2.10 There should be emphasis on importance of implementing an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks to enable effective management of those risks as illustrated in Figure1 below.

**Figure 1: Cyber Resilience Components**

5.2.11 **Collaboration:** Effective solutions may necessitate collaboration between institutions and their stakeholders as they seek to strengthen their own cyber resilience. Efforts to coordinate the design of resilience solutions may bring enhanced strategies forward, in a timely and efficient way.

5.2.12 **Organisation and Resources:** Allocation of an adequate cybersecurity budget based on the institution’s structure and size of its cyber risk function.

5.2.13 **Cybersecurity Incident Management:** Cybersecurity incident response plan should provide a roadmap for the actions the institution will take during and after a security incident.

6 **GOVERNANCE AND BOARD OVERSIGHT**

6.1 Cybersecurity exists and is transformed, within the values and objectives of the enterprise and its members. Cybersecurity is a joint or collective operation as well as everyone’s responsibility.

6.2 As such, cybersecurity is a subject to clear governance rules that provide a sense of direction as well as reasonable boundaries.

6.3 The ultimate responsibility for cyber security rests with the board of the institution and includes adopting and improving the organizational governance framework for cybersecurity.
6.4 **The Board**

6.4.1 The Board of Directors are charged with the responsibility of setting an institution's risk management policies, including its cybersecurity policy. In order to achieve this, the Board should collectively understand the nature of the institution’s business, vulnerabilities and cyber threats arising from the operating environment.

6.5 **Board Responsibility for cyber-resilience.**

6.5.1 The board of directors of an FMI, PSP and participant bank are charged with overseeing the institution’s financial systems and controls including the management of cybersecurity, oversight of appropriate risk mitigation strategies, systems, processes and controls.

6.5.2 The board and senior management of an institution are expected to formulate and implement cybersecurity strategies, policy, procedures, and guidelines and set minimum standards for an institution. All these must be documented and made available for review by external auditors and Central Bank supervisors or any other relevant regulatory bodies.

6.5.2.1 The board as a whole takes ultimate responsibility for oversight of cyber-risk and resilience.

6.5.2.2 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).

6.6 **Board Oversight**

6.6.1 Effective oversight, collaboration and cooperation on cyber risk matters at the board level promotes a risk conscious culture within the institution.

6.6.1.1 Among others, the oversight responsibilities of the board in relation to cyber risk should include the following key aspects:

i. Setting “the right tone from the top” is a crucial element in fostering a robust cyber risk management culture;

ii. Ensure that the cyber security policy is approved by the Board and aligns with the overall business strategy;

iii. Continuous cultivation and promotion of an ethical governance and cyber management culture supported by education and awareness programs;

iv. Establish the institution’s vision, risk appetite and overall strategic direction with regards to cybersecurity.

v. Ensure adequate cybersecurity budget based on the institution’s level of activities and strategic direction.

vi. Ensure that the cybersecurity policy applies to all of the institution’s operating entities, including subsidiaries, joint ventures and geographic regions.

vii. Incorporate cybersecurity as a standard agenda in Board meetings.

viii. Ensure that, cybersecurity policy incorporates monitoring metrics coupled with reporting and trend analysis.

ix. Review and approve ICT strategic plan that aligns with the overall business strategy.

6.7 **Board Command of the Subject.**

6.7.1 Board members receive cyber-resilience orientation on joining the board and are regularly updated on recent threats and trends.
6.8 **Chief Information Security Officer (CISO).**

6.8.1 The board ensures that the CISO is accountable for reporting on the organisation’s capability to manage cyber-resilience and progress in implementing cyber-resilience goals. The board ensures that this officer has regular access to the board, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

6.9 **Integration of cyber resilience.**

6.9.1 The board ensures that management integrates cyber-resilience and cyber-risk assessment into the overall business strategy and enterprise-wide risk management, as well as budgeting and resource allocation.

6.10 **Risk appetite.**

6.10.1 The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite.

6.11 **Risk assessment and reporting.**

6.11.1 The board holds management accountable for reporting a quantified and comprehensible assessment of cyber-risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber-Risk Framework.

6.12 **Resilience Plans.**

6.12.1 The board ensures that management supports the CISO (Chief Information Security Officer) by the creation, implementation, testing and ongoing review of cyber-resilience plans, which are aligned to the institution’s assessed cyber risk exposure across all business lines.

6.12.2 The CISO shall be required to monitor the performance of the institution’s cyber resilience plan and regularly reporting to the board by making relevant recommendations for its consideration.

6.13 **Collaborate and cooperation**

6.13.1 The board is responsible for establishing a framework for co-operation and information sharing between management of the institution and other relevant stakeholders, in order to ensure systemic cyber resilience.

6.14 **Review.**

6.14.1 The board is responsible for ensuring that a formal, independent cyber-resilience review of the organisation is carried out annually.

6.15 **Effectiveness.**

6.15.1 The board periodically reviews its own performance in the implementation of these strategies or seeks independent expert advice for continuous improvement.
6.15.2 The periodic reviews should ensure that:

6.15.2.1 BCPs of the institution’s cybersecurity preparedness is aligned with its requisite standards.
6.15.2.2 Any material changes to the institution’s products, services, policies or practices and threat landscape does not affect its cyber risk profile.
6.15.2.3 Effective internal cybersecurity control framework is maintained through submission of periodic independent reports to the board by the CISO. Institutions should determine the scope, comprehensive and frequency of independent reports from internal and external audit.
6.15.2.4 Cybersecurity risk ownership, coverage and management accountability are well established and not limited to information technology function.
6.15.2.5 Approvals and continuous reviews of the cybersecurity strategy, governance charter, policy and framework are conducted in an integrated manner. The strategy, policies and frameworks should be tailored based on the institution’s risk profile, size, complexity and nature of their business processes.
6.15.2.6 The results of management’s ongoing monitoring of the institution’s exposure to and preparedness for cyber threats are fully utilised to the benefit of the institution.

6.16 Executive Management

6.16.1 Management of an institution is responsible for implementing the institution’s business strategy, risk appetite and threats. Management is also responsible for closely overseeing the implementation of the institution’s cyber resilience framework, including the policies, procedures and controls that support.

6.16.2 Executive Management Responsibility;

6.16.2.1 Implementation of the board approved cybersecurity strategy, policy and framework.
6.16.2.2 Ensure understanding of organizational cyber risk profile through the identification of critical business processes assets and potential cyber threats.
6.16.2.3 Ensure the creation of mitigation and recovery procedures to contain cyber risk incidents, reduce losses and return operations to normal. In so doing, management should bear in mind that cyber risk is managed within the context of overall ICT risk management. Management should therefore ensure that cyber security considerations are incorporated into the institution’s Business Continuity Management (BCM) processes.
6.16.2.4 The BCP should clearly spell out strategies with regards to the Recovery Time Objective (RTO) and Recovery Point Objectives (RPO).
6.16.2.5 Continuously improve collection, analysis, and reporting of cybercrime information. This can be achieved through understanding the business environment institutions operate in, potential cyber risk points with reference to international best practices.
6.16.2.6 Oversee deployment of strong authentication measures to protect customer data, transactions and systems.
6.16.2.7 Ensure the provision of sufficient number of staff members with the appropriate skills and knowledge to understand as well as manage the risks posed by cyber threats, while ensuring that those skills remain current and relevant;
6.16.2.8 Ensure that staff members are subjected to enhanced background checking before being engaged and after;
6.16.2.9 Incorporate cybersecurity as a standard agenda in Senior Management and ICT steering committee meetings.
6.16.3 Oversee the evaluation and management of risks introduced by third party service providers; institutions may require attestation/assurance reports provided by reputable independent auditors for service providers. Service Level Agreements should provide for institutions to have access to the audit reports on an on-going basis, and the following measures should apply:

6.16.3.1 Ensure timely and regular reporting to the board on the cyber risk status of the institution.
6.16.3.2 Establish a cybersecurity benchmarking framework with the Board’s endorsement.
6.16.3.3 Promote a culture that recognises that staff at all levels have important responsibilities in ensuring the institution’s cyber resilience.
6.16.3.4 Provide regular reports of the institution’s cybersecurity posture to the board.
6.16.3.5 Document cybersecurity incident response plan providing a roadmap for the actions the institution will take during and after a security incident. The plan should address inter-alia:
   • The roles and responsibilities of staff;
   • Recovery/Return Time Objectives;
   • Recovery/Return Point Objectives;
   • Incident detection and assessment, reporting;
   • Periodic Incident Recovery Tests; and
   • Escalation and strategies deployed.
6.16.3.6 Collaborate with other institutions and the security agencies to share the latest cyber threats/attacks encountered by the institution.
6.16.3.7 Create a post incident analysis framework to determine corrective actions to prevent similar incidents in the future.

6.17 The CISO is Responsible for:

6.17.1 Oversight and implementing the institution’s cybersecurity program and enforcing the cybersecurity policy.
6.17.2 Day to day cybersecurity activities and the mitigation of cybersecurity risk. Ensuring that the institution maintains a current enterprise-wide knowledge base of its users, devices, applications and their relationships, including but not limited to:
   • Software and hardware asset inventory;
   • Network maps (including boundaries, traffic and data flow); and
   • Network utilization and performance data.
6.17.3 Ensuring that information systems meet the needs of the institution, and the ICT strategy, in particular information system development strategies, comply with the overall business strategies, risk appetite and ICT risk management policies of the institution.
6.17.4 Identify and maintain a current log of both individual and system credentials particularly relating to access rights to information assets and their supporting systems. Review system access and activities for identification and investigation of anomalous activities.
6.17.5 Design cybersecurity controls with the consideration of users at all levels of the organization, including internal (i.e. management and staff) and external users (i.e. contractors/consultants, business partners and service providers).
6.17.6 Conduct ongoing professional cybersecurity related training to improve technical proficiency of staff.
6.17.7 Ensure that regular and comprehensive cyber risk assessments are conducted.
6.17.8 Ensure that adequate processes are in place for monitoring ICT systems to detect cybersecurity events and incidents in a timely manner.

6.17.9 Reporting to the CEO on an agreed interval but not less than once per quarter on the following:
   - Assessment of the confidentiality, integrity and availability of the information systems in the institutions.
   - Detailed exceptions to the approved cybersecurity policies and procedures.
   - Assessment of the effectiveness of the approved cybersecurity program.
   - All material cybersecurity events that affected the institution during the period.

6.17.10 Ensure timely update of the incident response mechanism and Business Continuity Plan (BCP) based on the latest cyber threat intelligence gathered.

6.17.11 Incorporate the utilization of scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.

6.17.12 Ensure frequent data backups of critical ICT systems (e.g. real time back up of changes made to critical data) are carried out to a separate storage location.

6.17.13 Ensure the roles and responsibilities of managing cyber risks, including in emergency or crisis decision-making, are clearly defined, documented and communicated to relevant staff.

6.17.14 Continuously test disaster recovery and Business Continuity Plans (BCP) arrangements to ensure that the institution can continue to function and meet its regulatory obligations in the event of an unforeseen attack through cyber-crime.

6.17.15 **Regular Independent Assessment and Test**

6.17.15.1 The understanding of the cyber threat landscape within institutions requires a collaborative approach that encompasses the following functions such as the Internal and External Audit Risk Management.

6.17.15.2 Institutions should engage external consultants with sufficient cybersecurity expertise to assist in understanding their cyber threat landscape. Institutions should carry out an independent cyber threat test at least once a year.

6.17.15.3 Every institution shall establish an ICT steering committee that shall be responsible for the governance of the cyber security programme. The steering committee shall consist of senior representative of relevant departments within the institution. The roles, responsibilities, scope and activities of the information security steering committee shall be clearly defined in the terms of reference (TOR).

6.17.15.4 The objectives of the Committee shall include:
   - Ensuring that policies and processes align with the business objectives;
   - Providing strategic direction and cybersecurity governance for the institution;
   - Evaluating, approving, and sponsoring institution-wide security investment;
   - Enforcing the implementation of policies for investment prioritisation and security risk management.

6.18 **Role of Internal Auditors**

6.18.1 An FMI, PSP’s internal processes should help the board and senior management assess and measure the adequacy and effectiveness of its cybersecurity policy.
6.18.2 The adequacy of and adherence to an FMI, PSP’s cybersecurity policy should be assessed and measured regularly through independent compliance programmes and audits carried out by qualified individuals. All institutions are expected to incorporate qualified Information and Communication Technology (ICT) Auditors within the Internal Audit team as permanent staff or outsourced service.

6.18.3 All institutions should ensure that they incorporate cyber security reviews into the internal auditors plan for the institution.

6.19 **Role of External Auditors**

6.19.1 External auditors should ensure that the ICT audit scope includes and is not limited to:

6.19.1.1 Obtaining an understanding of the institution’s ICT infrastructure, use of IT, operations and the impact of ICT on financial reporting statements.

6.19.1.2 Understanding the extent of the institution’s automated controls as they relate to financial reporting. This should include an understanding of:

6.19.1.2.1 ICT general controls that affect the automated controls.

6.19.1.2.2 Reliability of data and reports used in the audit that are produced by the institution.

6.19.1.3 Comprehensive review of the approved cybersecurity strategy and policy.

6.19.1.4 Report annually as required to the board and the Reserve Bank of Zimbabwe on the findings of the assessments.
7 CYBERSECURITY RISK MANAGEMENT SYSTEM

7.1 Risk-Based Cyber Risk Management

7.1.1 The Guideline is risk based as it prescribes key cyber security principles and objectives to be embedded and achieved by the individual institutions.

7.1.2 An effective risk-based cybersecurity management program is based on good knowledge or understanding by the individual institution of the threats and vulnerabilities in the ecosystem. When control measures cannot be tailored or implemented, the individual institution (payment services providers and banks) should consider applying compensating controls, pursuing an internal risk acceptance.

7.1.3 Accordingly, the board has the ultimate role in defining the risk appetite of the financial institution and ensure there is a risk management framework in place to identify and effectively manage cyber risks on an ongoing basis. Refer to Section 6 of this Guideline.

7.1.4 Management of the institution’s exposure to cyber risk is determined by an assessment of the inherent exposure to cyber risk in the execution of its business strategy.

7.2 Effective Risk Management

7.2.1 Effective Risk Management serves to reduce the incidence of significant adverse impact on an organization by addressing threats, mitigating exposure, and reducing vulnerability. FMIs, PSPs and participating banks shall incorporate cyber-risk management with their institution-wide risk management framework and governance requirements to ensure consistent management of risk across the institution.

7.2.2 Cybersecurity risk management should be continuous and proactive, requiring oversight, not only of the technology, but also of the people and the processes that use and support the technology.

7.2.3 The process shall also be dynamic in view of the constantly changing risk landscape.

7.2.4 The institution’s cyber security risk management should support financial stability objectives while ensuring the ongoing efficiency, effectiveness and economic viability of its services to its users.

7.2.5 Critically important is for the institution to implement cyber controls whilst at the same time balancing the costs against the benefits. As an example, the institution should have in place security operation centres, incident response teams or forensic investigations capabilities which can be available in-house or be outsourced.

7.2.6 Therefore, the objectives should aim to maintain and promote the institution’s ability to anticipate, withstand, contain and recover from cyber-attacks, so as to limit the likelihood or impact of a successful cyber-attack on its operations or on the broader financial system.

7.2.7 The Board and Senior Management shall support and be involved in the cyber-risk management process by ensuring that resources and capabilities are available and roles of staff properly defined in management of risks.
7.2.8 The Risk Management System shall cover at least the five basic activities which are largely covered in many international standards, regulations and guidelines as below:

i. Risk Identification
ii. Risk assessment
iii. Risk measurement
iv. Risk mitigation/Risk treatment...and
v. Risk Understanding
8 ROLE OF RISK MANAGEMENT FUNCTION

8.1 This comprises risk control and compliance oversight functions which ultimately ensure that an institution’s management of data, processes, risks, and controls are effectively operating. Risk management has the duty to ensure that cybersecurity risks are managed within the enterprise risk management portfolio (as a dedicated category or as a subset of the operational risk).

8.2 An FMI and participant bank should take an integrated and comprehensive view of the potential cyber threats it faces.

8.3 In particular, it should consider how the institution would regularly review and actively mitigate the cyber risks that it bears from and poses to its participants, other FMIs, vendors, vendor products and its service providers, which are collectively referred to in this document as an FMI, PSP’s ecosystem.

8.4 The institution’s risk management function should include and is not limited to the tasks below:

8.4.1 Assessing the risks and exposures related to cybersecurity and determining whether they are aligned to the institution’s risk appetite.

8.4.2 Monitoring current and emerging risks and changes to laws and regulations that may impact on the level of cyber risk exposure in the institution.

8.4.3 Collaborating with system administrators and others charged with safeguarding the information assets of the institution to ensure appropriate control design.

8.4.4 Clearly define the roles and responsibilities including accountability for decision making within the organisation for managing cyber risk, including in emergencies and in a crisis.

8.4.5 Maintain comprehensive cyber risk registers: Key cybersecurity risks should be regularly identified and assessed. Risk identification should be forward looking and include the security incident handling.

8.4.6 Ensure implementation of the cyber and information risk management strategy.

8.4.7 Safeguarding the confidentiality, integrity and availability of information.

8.4.8 Ensure that a comprehensive inventory of ICT assets, classified by business criticality, is established and maintained. A Business Impact Analysis process is in place to regularly assess the business criticality of ICT assets.

8.4.9 Quantify the potential impact by assessing the residual cyber risk and considering risks that need to be addressed through insurance as a way of transferring cyber risk.

8.4.10 Reporting all enterprise risks consistently and comprehensively to the board to enable the comparison of all risks equally in ensuring that they are prioritized correctly.

8.4.11 Institutions are required to report all cyber incidents including registered threats within seven days of occurrence.
9.1 The Institutions should define, approve, implement and monitor a cyber-security standard for Digital Financial Services (DFS). To ensure the institution safeguards the confidentiality and integrity of the customer information and transactions including availability of critical systems.

9.2 **DFS Key Considerations:**

9.2.1 The cyber security standards for DFS should be defined, approved and implemented.

9.2.2 The compliance with cyber security standards for DFS should be monitored.

9.2.3 The effectiveness of the cyber security standard for DFS should be measured and periodically evaluated.

9.2.4 Furthermore, use of multi-factor authentication mechanisms should be guided by password policy as follows:

9.2.4.1 Multi-factor authentication should be used during the registration process for the customers to enable them to use online facilities or services;

9.2.4.2 Multi-factor authentication should be implemented for all electronic banking and financial services available to customers;

9.2.4.3 The use of hard and soft tokens should be password protected;

9.2.4.4 Revoking of customer’s access after successive incorrect passwords or invalid PINs;

9.2.4.5 The process for changing the customer mobile number should be done from a branch, ATM; or using a two-step verification process (for example a change in mobile number may use e-mail verification and a token ID to have the change effected or a push notification on the customer device);

9.2.4.6 The processes for requesting and activating of the multi-factor authentication should be done through different delivery channels;

9.2.4.7 Multi-factor authentication should be implemented for the following processes:

a) sign-on;

b) adding or modifying beneficiaries;

c) adding utility payment services;

d) high-risk transactions (when it exceeds predefined limits);

e) password reset;

f) the processes for adding and activating beneficiaries should be done through different delivery channels (applicable for mobile payments and online banking);

g) high availability of the DFS should be ensured;

9.3 **SMS instant notification services:**

9.3.1 SMS messages should not contain sensitive data;

9.3.2 SMS alert should be sent to both mobile numbers (old and new) when the customer’s mobile number has been changed and e-mail;

9.3.3 SMS notification should be sent to the customer’s mobile number when requesting a new multi-factor authentication mechanism or e-mail.
10 TRAINING/Awareness

10.1 Institutions should implement ICT security awareness training programmes to provide information on good IT security practices, common threat types and the institution’s policies and procedures. The training should be provided to all employees including senior management and the board.

10.2 A formalized plan should be put in place to provide ongoing technical training to cybersecurity specialists within the institution.

10.3 Cybersecurity awareness and information should be provided to the institution’s customers, clients, suppliers, partners, outsourced service providers and other third parties who have links to the financial institution’s ICT infrastructure.

10.4 Insider threats

A financial institution should implement measures to capture and analyse anomalous behaviour by persons with access to its systems.

10.5 Data loss identification and prevention techniques should be employed to protect against the removal of confidential data from the institution’s network.

10.6 An institution should conduct screening/background checks on new employees to mitigate insider threats. Similar checks should be conducted on all staff at regular intervals throughout their employment, commensurate with staff’s access to critical systems.

10.7 Financial institutions should establish processes and controls to mitigate risks related to employees terminating employment or changing responsibilities. Physical and logical access to systems should be permitted only for individuals who are authorised, and authorisation should be limited to individuals who are appropriately trained and monitored.

10.8 FMIs and participant banks should institute controls that reliably restrict such access to systems to those with a legitimate business requirement. In particular, FMIs should institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements.

10.9 Controls such as roles-based access, logging and reviewing of the systems activities of privileged users, strong authentication, and monitoring for anomalies should be implemented.
11 SUBMISSIONS OF REPORTS

11.1 All institutions are required to review and submit their cybersecurity strategy, policy, and frameworks that they subscribe to regularly or annually based on each institution’s threat and vulnerability assessment.

11.2 The institutions should notify the Reserve Bank of Zimbabwe within 24 hours of any cybersecurity incident(s) that could have a significant and adverse impact on the institution’s ability to provide adequate services to its customers, its reputation or financial condition.

11.3 On a quarterly basis, institutions shall provide Reserve Bank of Zimbabwe with a report concerning its occurrence and handling of cybersecurity incidents via the email address: npsd@rbz.co.zw.
In the event of any query or clarification, please contact:

The Deputy Director,
Financial Markets Division,
National Payment Systems
Reserve Bank of Zimbabwe (RBZ)
80 Samora Machel Avenue, Harare
Tel: +263242703000
Email: npsd@rbz.co.zw