REPUBLIC OF ZAMBIA

GOVERNMENT GAZETTE

Published by Authority

Price: K15.00 net
Annual Subscription: —K400.00

No. 7240] Lusaka, Friday, 19th May, 2023 [Vol. LIX, No. 30

GAZETTE NOTICE No. 668 OF 2023

[1112904

The Bank of Zambia Act
(Cap 360 of the Laws of Zambia)

The Banking and Financial Services Act, 2017

The National Payment Systems Act, 2007

The Credit Reporting Act, 2018

The Bank of Zambia Cyber and Information Risk Management Guidelines, 2023

PART I:

1 PRELIMINARY

IN EXERCISE of the powers contained in Section 167 (1) of the Banking and Financial Services Act (BFSA) No.7 of 2017, Section 43 (1) of the National Payment Systems Act (NPSA) No.1 of 2007 and Section 63 of the Credit Reporting Act of 2018, the following Guidelines are hereby made:

2 SHORT TITLE

These Guidelines may be cited as the Bank of Zambia Cyber and Information Risk Management Guidelines, 2023.

3 INTERPRETATION

In these Guidelines unless the context otherwise requires:

Asset – means the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes.

Availability – means information assets are resilient and accessible when required.

Bank – means the Bank of Zambia as established by the Bank of Zambia Act, Chapter 360 of the Laws of Zambia.

Business Continuity – refers to capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Business Continuity Plan – means 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 an event of a disruption.

Cloud computing – means service and delivery model for enabling on-demand network access to a shared pool of configurable computing resources (servers, storage, and services). "The cloud" refers to servers that are accessed over the Internet, and the software and databases that run on those servers.

Confidentiality – means information assets are only accessible by those authorised to have access.

Credit reporting agency – has the meaning assigned to the words in the Credit Reporting Act of 2018.

Critical information – has the meaning assigned to the words in The Cyber Security and Cyber Crimes Act of 2021.

Critical information infrastructure – has the meaning assigned to the words in The Cyber Security and Cyber Crimes Act of 2021.

Cyber – has the meaning assigned to the words in The Cyber Security and Cyber Crimes Act of 2021.

Cyber and Information Security – means the protection of cyber and information assets by addressing threats to information processed, stored, and transported by internetworked information systems.

Cyber and information security incident – has the meaning assigned to the words in The Cyber Security and Cyber Crimes Act of 2021.

Cyber Attack – means an attempt to gain unauthorized access to a computer, computing system, or computer network for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure.

Cybercrime – has the meaning assigned to the words in the Cyber Security and Cyber Crimes Act of 2021.

Cyber security – has the meaning assigned to the words in The Cyber Security and Cyber Crimes Act of 2021.

Data – means pieces of information from which "understandable information" is derived.

Financial service provider – has the meaning assigned to the words in the Banking and Financial Services Act (BFSA) No.7 of 2017.

Information – means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual.

Integrity – means the property that data or information have not been altered or destroyed in an unauthorized manner.

Internal Controls – Means a process effected by a regulated entity's board of directors, management and staff designed to provide reasonable assurance regarding the achievement of objectives such as effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations.

Material Outsourcing – means outsourcing arrangements, which if disrupted, have the potential to significantly impact the business operations, reputation or profitability of a regulated entity.

Payment System - has the meaning assigned to the words in the National Payment Systems Act (NPSA) No.1 of 2007.

Payment System Business – has the meaning assigned to the words in the National Payment Systems Act (NPSA) No.1 of 2007.

Regulated entity - Means a financial service provider, payment system, payment system business, and credit reference agency.

Risk appetite – Means the aggregate level and types of risk a regulated entity is willing to assume, decided in advance and within its risk-taking capacity, to achieve its strategic objectives and business plan.

Threat – means any circumstance or event with the potential to adversely impact regulated entity operations.

Virtualisation – means the simulation of the software or hardware upon which other software runs. This simulated environment is called a virtual machine.

Vulnerability – means weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

4 APPLICATION

The Bank is cognisant of the differences in the nature, size, and complexity of regulated entities. In this regard, these Guidelines are issued on an apply or explain approach with the expectation that bigger and more complex entities will fully apply the Guidelines. The entities that will not be able to apply all the guidelines are required to provide an explanation on how they manage the cyber and information risk that they are exposed to in the pursuit of their business objectives. The Guidelines shall apply to all Regulated Entities.

PART II

5 PREAMBLE

The technology landscape of the financial sector is transforming rapidly and the underlying information technology (IT) infrastructure supporting financial services has evolved in scope and complexity. Regulated entities are leveraging on digital platforms to increase operational efficiency and to deliver better services. The increased dependence on digital platforms exposes regulated entities to cyber and information risk. There is, therefore, a need for regulated entities to strengthen their technological resilience against operational disruptions to maintain confidence in the financial system. These Guidelines outline the Bank of Zambia's (the Bank) minimum requirements regarding the regulated entities management of cyber and information risk.

The Guidelines cover five cyber and information risk control areas namely Identify, Protect, Detect, Respond and Recover anchored on the National Institute of Standards and Technology (NIST).

6 PURPOSE OF GUIDELINES

The purpose of these Guidelines is to prescribe minimum requirements to regulated entities on cyber and information risk management.

PART III

7 CYBER AND INFORMATION RISK GOVERNANCE

Cyber and information risk governance is one of the core components of the Cyber and Information Risk Framework which sets the program for cyber and information risk management and controls. The overall Cyber and Information Risk Framework should include clearly defined responsibilities for the management of cyber and information risk across the regulated entity with an appropriate risk management structure to ensure that the risk is within the parameters set by the board. The structure should be commensurate with the size, complexity, and diversity of the entity's activities.

In addition, the structure should facilitate effective board and senior management oversight and proper execution of risk management and control processes. At a minimum, the risk governance structure should include board of directors, board risk management committee, senior management, management risk committees, risk management function and chief information security officer. The Bank therefore expects the regulated entity to ensure the following are implemented:

7.1 ROLES AND RESPONSIBILITIES OF THE BOARD

The regulated entity's board shall:

1. Set a tone from the top and cultivate a strong culture of risk awareness that emphasizes and demonstrates the importance of cyber and information risk management.
2. Provide direction to senior management on what cyber resilience should achieve.
3. Establish appropriate cyber and information risk management governance structures.
4. Establish and implement a cyber and information risk management strategy.
5. Approve the risk appetite and tolerance for cyber and information risk considering the risk landscape.
6. Provide senior management responsible for executing the cyber and information risk management strategy, sufficient authority, and resources.
7. Approve the cyber and information risk management framework and ensure that cyber and information risk is effectively managed.
8. Review and approve work plans for cyber and information risk, business continuity and disaster recovery.
9. Approve and communicate the cyber and information risk management policies.
10. Regularly review cyber and information risk management policies and strategies.
11. Provide oversight in the implementation of internal controls and risk management practices.
12. Review the reports on performance and outcomes of cyber resilience and provide intervention where necessary including policy direction.
13. Ensure that measures are put in place for collaboration and information sharing on cyber and information risk incidents with relevant stakeholders.
14. Consider material changes to the regulated entity's products, services, policies, or practices, and how the threat landscape affects its cyber risk profile.

7.2 ROLES AND RESPONSIBILITIES OF SENIOR MANAGEMENT

The regulated entity's senior management shall:

1. Implement the cyber and information risk management framework and strategy.
2. Establish an appropriate committee headed by a senior officer from a control function to effectively manage cyber and information risk.
3. Clearly assign and communicate the responsibilities and authorities for roles relevant to cyber and information risk management.
4. Regularly apprise the board of salient and adverse cyber and information risk developments and incidents that are likely to have a major impact on the regulated entity in a timely manner.
5. Have sufficient number of skilled staff for the management of cyber and information risk, who should be subjected to enhanced background checks.
6. Collaborate with relevant stakeholders to share cyber threats, incidents, and attacks that the regulated entity encountered.
7. Oversee the evaluation and management of cyber and information risks introduced by third party service providers. The regulated entity may require attestation/assurance reports provided by reputable independent auditors for service providers.
8. Designate an appropriately qualified senior officer as a Chief Information Security Officer (CISO) independent from day-to-day information technology operations to be responsible and accountable for executing the cyber and information risk management framework with sufficient authority and resources.
9. Determine the best reporting option of the CISO depending on factors, such as, vision and strategic goals, culture, management style, security maturity, IT maturity, risk appetite and all relevant dynamics involving the current security posture and reporting lines.
10. Assign the designated CISO with the responsibility to oversee and enforce cyber and information risk management policies, frameworks, and other technology-related regulatory requirements.
11. Monitor performance and outcomes of cyber resilience and intervene if necessary to ensure that specified direction is followed.
12. Review and assess risks associated with changes in the cyber and information risk landscape.
13. Establish a Security Operation Center (SOC) or at a minimum setup mechanism to monitor cyber and information security threats on an ongoing basis, and to promptly detect, analyse, and respond to cyber and information security incidents.
14. Cultivate a strong level of awareness of and commitment to cyber resilience by conducting comprehensive cyber and information risk awareness training programmes to its members of staff and other stakeholders.

7.3 POLICIES, STANDARDS AND PROCEDURES

The regulated entity shall ensure:

1. Policies for managing cyber and information risk are approved by the Board and regularly reviewed.
2. Policies cover the cyber and information risk threat environment and its potential impact, and the principles for implementing cyber and information risk measures.
3. Policies include the approach for managing cyber and information risk, and the mechanisms for determining and monitoring the level of exposure to threats.
4. Policies are consistent with relevant laws and regulations, as well as international cyber and information risk management standards and best practice.
5. Responsibilities and governance structures for cyber and information risk management are clearly outlined.
6. Policies include provisions for cyber and information risk awareness and training programmes for relevant stakeholders.
7. Policies include provisions for collaboration and information sharing arrangements within the regulated entity and other relevant stakeholders.
8. Cyber and information risk management policies are consistent with other risk management policies including business continuity management, outsourcing, emerging initiatives, and change management.
9. Specific and detailed procedures are developed to cover all cyber and information risk management related issues.
10. That senior management implement compliance processes to verify that information and cyber risk management policies and procedures are enforced.
11 Procedures are regularly reviewed and updated, taking into consideration the evolving cyber and information risk threat landscape.

PART IV

8 IDENTIFY

This process involves identification of information assets that support critical functions and assessment of threats and vulnerabilities to ensure that a regulated entity understands its cyber and information risk. This will enable a regulated entity to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

The Bank expects the regulated entity to undertake the following in identifying the cyber threats and attacks:

8.1 ASSET MANAGEMENT

The regulated entity shall ensure that:

1. The data, personnel, devices, systems, and facilities that enable the achievement of business purposes are identified and managed consistent with their relative importance to business objectives and the risk strategy.
2. Inventory of physical devices, applications and systems is maintained and updated regularly.
3. Third party information systems are catalogued.
4. Communication and data flows are mapped to cyber and information risk management roles and responsibilities for the entire workforce and relevant stakeholders.
5. Cyber and information risk management roles and responsibilities for the entire workforce and relevant stakeholders are established.

8.2 BUSINESS ENVIRONMENT

The regulated entity shall:

1. Understand its mission, objectives, stakeholders, and activities. These should be prioritized and communicated to all relevant stakeholders to inform its cyber and information risk management.
2. Identify and communicate its role in the supply chain to relevant stakeholders.
3. Identify and document all processes that are dependent on third-party service providers, its interconnections, and update this information on a regular basis.
4. Identify and communicate its role in critical information infrastructure and industry to the relevant stakeholders.
5. Establish dependencies and vital functions for delivery of critical services.
6. Establish resilience requirements by identifying dependencies and critical functions for delivery of critical.
7. Establish resilience requirements to support the delivery of critical services.
8. Maintain an up-to-date inventory of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections.

9. Create and maintain a network topology of all the existing infrastructure that support critical functions and identify external links.
10. Conduct risk assessments before deploying new and/or updated technologies, products, services, and connections to identify potential threats and vulnerabilities.
11. Maintain an inventory of all individual users, system accounts, privileged and remote access accounts, to be aware of the access rights to information assets and supporting systems.
12. Put in place mechanisms to ensure access to threat and vulnerability information -sharing sources.
13. Have capabilities in place to gather cyber and information risk threat information from internal and external sources such as application, system, network logs and security products.
14. Gather, analyse, continuously review intelligence data on cyber and information threats, and update with new threats and vulnerabilities. The risk reports should be submitted to the Board and senior management to facilitate risk management.
15. Incorporate lessons learned from its analysis of cyber and information risk, into the employee training and awareness programmes.

8.3 RISK ASSESSMENT

The regulated entity shall:

1. Understand the cyber and information risk to operations including mission, functions, image or reputation, assets, and stakeholders.
2. Identify and document asset vulnerabilities, threats both external and internal, determine the likelihood and impact of risks and assign appropriate risk responses to identified risks.
3. Conduct regular assessments on the effectiveness of the control environment in addressing cyber and information risks and determine any residual risks.
4. Have an enterprise risk management framework to identify risks and conduct risk assessments on a regular basis and of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections to determine, classify and document their level of criticality.
5. Revise risk assessments of cyber and information risks and the control infrastructure in accordance with the changes and trends in the threats and vulnerability landscape.
6. Identify existing and emerging cyber and information risk vulnerabilities and threats pertaining to critical and sensitive information assets and implement remedial measures in a timely manner.
7. Conduct risk assessments before deploying new and/or updated technologies, products, services, and connections to identify potential threats and vulnerabilities.
8. Document cyber and information risk identification, measurement and assessment methodologies which should be approved by senior management.
9. Report information obtained from risk assessment activities to senior management and the board to support informed decision-making.

8.4 CYBER AND INFORMATION RISK MANAGEMENT

The regulated entity shall:

1. Establish an Enterprise Risk Management Framework for the management of cyber and information risks in accordance with the three lines of defence principle.
2. Ensure that the first line of defence manages cyber and information risks in its day-to-day operations.
3. Have a function with cyber and information risk management expertise that provides control and compliance oversight to the first line of defence.
4. Establish an internal audit function that is adequately resourced and has relevant technology audit competencies to provide assurance over cyber and information risk and where inadequate, the board shall consider using external independent auditors.
5. Conduct cyber and information audits commensurate with the complexity, sophistication and criticality of systems and applications at a planned interval.

PART V

9 PROTECT

This process involves the implementation and maintenance of safeguards aimed at containing the impact of cyber and information risk events. This is to preserve the confidentiality, integrity, and availability of the regulated entity's information assets.

The Bank expects the regulated entity to undertake the following in protecting cyber threats and attacks:

9.1 ACCESS CONTROL

9.1.1 IDENTITIES AND CREDENTIALS

At a minimum, the regulated entity shall:

1. Design access controls to minimize potential cyber and information risk exposure resulting from unauthorized use of resources.
2. Provide unique identifiable credentials to all users, devices, and systems that access information assets.
3. Issue, manage, verify, revoke and audit identities and credentials for authorized users, devices, and processes.
4. Grant access rights and system privileges according to the roles and responsibilities of staff, contractors, service providers and other relevant stakeholders.
5. Apply the principles of 'never alone', 'segregation of duties', and 'least privilege' when granting access to information assets.
6. Implement job rotation and cross training for security administration functions.

9.1.2 PHYSICAL AND REMOTE ACCESS

At a minimum, the regulated entity shall:

1. Provide physical security of people, property, and assets, such as hardware, software, network, and data, from natural disasters, burglary, theft, terrorism, and other events that could cause damage or loss.
2. Establish physical security measures to prevent unauthorised access to systems and equipment.
3. Revoke access to all assets immediately it is no longer required.
4. Maintain an access log and limit access to the data centres to authorized persons only.
5. Secure and monitor the perimeter of the data centres, facilities, and equipment rooms.
6. Secure remote connections to prevent data leakage.
7. Implement strong user authentication for remote access, such as multi-factor authentication where appropriate to safeguard against unauthorised access to its systems.
8. Grant remote access to authorised devices that have been secured according to approved security standards.
9. Secure and maintain the logs of all remote connections to facilitate audit trail.

Protect logging facilities and log information against tampering and unauthorized access.

9.1.3 ACCESS PERMISSIONS AND AUTHORISATIONS

At a minimum, the regulated entity shall:

1. Apply stringent selection criteria and thorough screening when appointing staff to perform critical operations and security functions.
2. Monitor staff with elevated system access entitlements and have all their systems' activities logged and reviewed.
3. Restrict privileged users from accessing system logs in which all activities are captured.
4. Prohibit third parties from gaining access to systems without authorization, close supervision, and monitoring, and restrict access in line with service level and non-disclosure agreements.
5. Protect backup data from unauthorised access.
6. Perform regular reviews of user access privileges to verify that appropriate rights are granted according to the 'least privilege' principle.
7. Enforce strong password controls across its applications and systems.

9.1.4 NETWORK INTEGRITY

At a minimum, the regulated entity shall:

1. Install network security devices, such as, firewalls to secure the network between the regulated entity and the Internet, as well as connections to third parties.
2. Deploy intrusion prevention systems in its network to detect and block malicious activities.
3. Implement network access controls to detect and prevent unauthorised users and devices from connecting to its network.
4. Regularly review network access control rules for network devices, such as, firewalls, routers, switches, and access points to ensure they are in line with the security policy and best practice.
5. Isolate critical business system environment from its general-purpose system environment using physical and logical controls, or equivalent controls.
6. Review its network architecture, including the network security design, as well as system and network interconnections, on a periodic basis.

9.1.5 SYSTEMS SECURITY

The regulated entity shall:

1. Outline security baseline configurations of hardware and software which should be reviewed regularly for relevance and effectiveness.
2. Uniformly apply security standards on all systems and identify deviations, and address risks in a timely manner.
3. Implement appropriate endpoint protection solutions to protect the regulated entity from malware infection and address common delivery channels of malware.
4. Ensure that anti-malware solutions are kept up-to-date, and the systems are regularly scanned for malicious files or abnormal activities.
5. Implement security measures, such as, application whitelisting to ensure only authorised software is installed on the systems.
6. Conduct a risk assessment and implement appropriate measures to secure its Bring-Your-Own-Device (BYOD) environment before allowing staff to use their personal devices to access the regulated entity network.
7. Formulate a BYOD strategy/policy to govern the management of personal devices connected to the network.

9.1.6 VIRTUALISATION SECURITY

This process involves simulation of software or hardware upon which other software runs. The simulated environment is called a virtual machine (VM). Regulated entities using virtualisation to optimise the use of computing resources and to enhance resilience by allowing several virtual machines (VMs) to support different business applications hosted on a single physical system should manage contagion impact on other VMs should there be a system failure or security breach in one of the VMs.

The regulated entity shall:

1. Establish security standards for all components of a virtualisation solution.
2. Restrict administrative access to the virtual environment infrastructure.
3. Develop policies and procedures to manage virtual images and snapshots. These shall include details that govern the security, creation, distribution, storage, use, retirement and destruction of virtual images and snapshots.

9.1.7 SECURITY OF DIGITAL SERVICES

A regulated entity offering digital financial services should be aware of its unique risks and put in place additional measures aimed at addressing such risks.

The regulated entity shall:

1. Maintain customer and counterparty information, and transactions with utmost confidentiality and integrity.
2. Minimise disruption and ensure reliability of services delivered via digital channels.
3. Maintain critical digital financial services in high availability with reasonable response time to customer requests.
4. Authenticate users or devices and the authorisation of transactions.
5. Monitor anomalous transactions and ensure audit trail.
6. Encrypt all confidential information prior to transmission over the network for both client and host application systems.
7. Request users to verify details of the transaction prior to execution.
8. Secure user and session handling management.
9. Be able to capture the origin and destination of each transaction.
10. Provide timely notification to sender/receiver that is sufficiently descriptive of the nature of the transaction.
11. Bind the Multi-Factor Authentication (MFA) solution to the customer's account.
12. Notify customers of any activation and changes to the MFA solution via the customers' verified communication channel, in a timely manner.
13. Prompt a payer/sender to confirm details of the identified beneficiary and amount of any transaction.
14. Authenticate the code generated by payer/sender that should be specific to the confirmed identified beneficiary and amount.
15. Provide a convenient means for customers to promptly suspend their account in an event of suspected fraud.
16. Provide its customers with adequate notices of the safeguards.
17. Clearly define and understand its responsibilities and those of its service providers in the digital financial services arrangements.
18. Retain sufficient and relevant digital service transaction logs for investigations and forensic purposes in line with relevant laws and regulations.

9.1.8 CHANGE AND PATCH MANAGEMENT

A regulated entity must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems.

The regulated entity shall:

1. Continuously monitor and implement latest patch releases in a timely manner.
2. Test patches before applying to production.
3. Identify critical technology systems that are approaching EOL for further remedial action.
4. Put in place a change management framework to ensure that only authorized changes are applied.
5. Identify and conduct risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems.
6. Specify turnaround time for deploying patches according to the severity of the patches; and
7. Adhere to the workflow for end-to-end patch deployment processes including approval, monitoring, and tracking of activities.

9.1.9 OUTSOURCING FUNCTIONS TO THIRD PARTIES

A regulated entity in considering the use of a third party to perform some of its functions, must fully understand the inherent risks and the requirements of relevant laws and regulations.

The regulated entity shall:

1. Conduct a comprehensive risk assessment, due diligence and seek approval from the Bank prior to engaging in a material outsourcing arrangement.
2. Define, implement, and monitor cyber and information security controls for outsourced functions in line with approved policy.
3. Periodically measure and evaluate the effectiveness of the defined cyber and information risk controls for an outsourced service or function.
4. Logically segregate data held by a third party in the cloud from other data held by the cloud service provider.
5. Implement business continuity requirements in accordance with the approved policy.
6. Retain the right to audit and/or access to appropriate assurance reports on cyber and information risk controls.
7. Include provisions in service level agreements with third parties that facilitate review of cyber and information risk controls of the third-party service provider.
8. Include provisions in the agreements with the third-party service providers for the return of data and irreversible deletion of the data on termination of the relationship.
9. Clearly define and understand its responsibilities and that of the service provider in outsourcing arrangements.
10. Implement appropriate safeguards on customer and counterparty information, and proprietary data when using outsourcing services to protect against unauthorised disclosure and access.
11. Include provisions for safeguarding information in contracts for all outsourcing arrangements with critical IT service providers.
12. Include cyber and information risk assessment as part of due diligence process for outsourcing arrangements with critical IT service providers, including related subcontracting arrangements.

9.1.10 TESTING

To promptly identify all vulnerabilities and cyber and information risk to operations and IT assets.

The regulated entity shall:

1. Implement a vulnerability testing management strategy approved by the Board.
2. Conduct vulnerability assessment at least quarterly or when there is a significant change to the regulated entity's information processing infrastructure or when vulnerabilities are made known.
3. Conduct annual intelligence-led penetration tests on its internal and external network infrastructure as well as critical systems. The penetration testing shall reflect extreme but plausible cyber-attack scenarios based on emerging and evolving threat scenarios.
4. Engage suitably accredited penetration testers and service providers to perform this function.
5. Document and escalate the outcome of the penetration testing exercise to senior management in a timely manner to identify and monitor the implementation of relevant remedial actions.
6. Test backups periodically and according to the entity's policy.
7. Regularly test response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) in accordance with the entity's policy.
8. Test detection processes during development, implementation and on an ongoing basis.
9. Analyze and record lessons of all tests, to inform changes to the strategy and framework going forward.

9.2 AWARENESS AND TRAINING

9.2.1 AWARENESS PROGRAMME

At a minimum, the regulated entity shall:

1. Have a cyber and information risk management awareness programme and appraise staff, contractors, service providers and other relevant stakeholders on an ongoing basis.
2. Implement a Cyber and information risk management awareness programme that tailored to address the different target groups through multiple channels.
3. Evaluate the Cyber and information risk management awareness programme to measure their effectiveness and identify areas that require improvement.
4. Include a listing of suggested cyber and information risk management mechanisms and strategies needed to mitigate risks in the awareness programmes.

9.2.2 TRAINING

The regulated entity shall:

1. Provide continuous training to ensure that staff are competent to operate the regulated entity's systems securely, and address and apply cyber and information risk management controls.
2. Provide security-related skills training to staff in relevant functional categories in line with their job descriptions.
3. Provide training to the board, senior management, and relevant third parties to understand their cyber and information risk roles and responsibilities.

9.3 INFORMATION AND DATA SECURITY

The regulated entity shall:

1. Implement information and data security controls to prevent unauthorised access and data corruption.
2. Classify information and data in line with the regulated entity's data classification scheme.
3. Maintain an inventory of all sensitive information stored, processed, or transmitted by the regulated entity's technology systems, including those located on-site, off-site or at a remote service provider.
4. Implement cryptographic mechanisms to protect sensitive or confidential data stored on all devices including data at rest and in transit.
5. Formally manage information assets throughout their lifecycle.
6. Destroy sensitive information before electronic devices are disposed of.
7. Implement mechanisms to protect against data leaks.
8. Put in place checking mechanisms to verify software integrity.
9. Separate the development and test environment(s) from the production environment.

9.4 INFORMATION AND DATA PROTECTION PROCESSES AND PROCEDURES

The regulated entity shall:

1. Define, approve, and implement cyber and information risk management policies and procedures for information protection aligned with the organization's data protection needs, to identify, respond to and recover from cyber and information risk incidents.
2. Periodically measure and evaluate the effectiveness of the information security policies and procedures.
3. Conduct and maintain backups, both off-site and on-site.
4. Implement System Development Life Cycle to manage systems.
5. Put in place configuration change control processes.
6. Comply with policies and procedures regarding the physical operating environment for assets.
7. Continuously improve cyber and information protection processes.
8. Share effectiveness of protection technologies with relevant stakeholders.
9. Put in place and manage response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery).
10. Develop and implement a vulnerability management plan.
11. Destroy data according to policy.
12. Include cyber and information security in human resources practices such as deprovisioning and personnel screening.

9.5 MAINTENANCE AND REPAIR OF ASSETS

The regulated entity shall:

1. Maintain and repair assets consistent with policies and procedures.
2. Maintain and repair assets in a timely manner, with approved tools, and ensure that this is logged.
3. Maintain equipment in line with manufacturers' recommendations to ensure its continued availability and integrity.
4. Agree and document the cyber and information risk management requirements for mitigating the risks associated with service provider's access to assets.
5. Regularly monitor, review, and audit third-party service delivery.
6. Approve and log remote maintenance of assets in a manner that prevents unauthorized access.
7. Manage changes to the provision of services by third parties in line with the criticality of information, systems and processes involved, and risk assessment.

9.6 PROTECTIVE TECHNOLOGY

The regulated entity shall:

1. Manage technical security solutions to ensure the security and resilience of systems and assets are consistent with related policies, procedures, and agreements.
2. Maintain and regularly review event logs used for recording user activities, exceptions, faults, and security incidents.
3. Protect logging facilities and log information against tampering and unauthorized access.
4. Log, protect and regularly review system administrators and operators' activities.
5. Synchronize the clocks of all relevant information processing systems or security domains to a single reference time source.
6. Plan and agree audit requirements and activities involving verification of operational systems to minimize disruptions to business processes.
7. Protect and restrict use of removable media according to policy.
8. Implement procedures for the management of removable media in accordance with the information classification scheme.
9. Securely dispose of media using formal procedures.
10. Protect media containing information against unauthorized access, misuse, or corruption during transportation.
11. Implement a clean desk policy for papers, and removable storage media and adopt a clear screen policy for information processing facilities.
12. Protect communication and control networks including information in networks and its supporting processing facilities.
13. Segregate groups of information services, users, and information systems on networks.
14. Establish and maintain a policy for network security based on risk assessments and business requirements.
15. Implement network traffic filtering mechanisms, such as firewalls and intrusion detection software, with appropriate policies to control inbound and outbound traffic.
16. Encrypt information in transit and at rest in accordance with its classification.
17. Apply approved security protocols to network connectivity.
18. Establish trusted mechanisms to support secure transmission and receipt of information.

PART VI

10 DETECT

This process involves timely detection of occurrence of anomalies and events to implement appropriate countermeasures against potential breaches and facilitate proactive containment of actual breaches.

The Bank expects the regulated entity to undertake the following in detecting the cyber threats and attacks:

10.1 ANOMALIES AND EVENTS

The regulated entity shall:

1. Detect anomalous activities in a timely manner and the impact of such events is understood.
2. Establish a baseline of network operations and expected data flows for users and systems.
3. Analyze detected events to understand the areas attacked and methods used.
4. Aggregate and correlate multiple sources and sensors of event data to establish the occurrence of a breach.
5. Investigate events and triage incidents based on the sensitivity of data and assets involved.
6. Establish incident alert thresholds.

10.2 SECURITY CONTINUOUS MONITORING

The regulated entity shall

1. Monitor information assets to identify cyber and information risk events and verify the effectiveness of protective measures.
2. Monitor network in a timely manner to detect potential cyber and information security events.
3. Prevent personnel performing day-to-day IT operations from having write and delete privileges for event logs.
4. Mirror event logs in real time to a separate system and reviewed by personnel independent from the IT operations in a timely manner.
5. Monitor the physical environment to detect potential cyber and information risk events.

6. Monitor privileged account activity to detect potential cyber and information risk events.
7. Detect malicious code and unauthorized mobile code.
8. Monitor external service provider activity to detect potential cyber and information risk events.
9. Monitor unauthorized personnel, connections, devices, and software.
10. Perform vulnerability scans.

10.3 DETECTION PROCESSES

The regulated entity shall:

1. Define and allocate cyber and information risk management roles and responsibilities for accountability.
2. Implement detection mechanisms and appropriate procedures for compliance with laws, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
3. Communicate event detection information to appropriate parties in a timely manner to limit the magnitude of loss from cyber and information related risk events.
4. Continuously improve detection processes to keep pace with changes in the cyber and information risk management landscape.
5. Impose staff vacations or job rotations to detect improper or illegal activities.

PART VII

11 RESPOND

This process involves the establishment of a cyber and information risk incident response and management plan to expeditiously isolate and neutralise threats to reduce damage, recovery time and incident costs. The cyber and information risk incident management plan outlines communication, coordination, and response procedures to address plausible cyber and information threat scenarios.

The Bank expects the regulated entity to undertake the following in responding to cyber threats and attacks:

11.1 RESPONSE PLANNING

The regulated entity shall:

1. Execute and maintain processes and procedures to ensure timely response to detected cyber and information risk events.
2. Define, approve, implement, and align the cyber and information risk incident management process with the enterprise incident management process.
3. Periodically measure and evaluate the effectiveness of the controls within the cyber and information risk incident management process.
4. Include the following requirements in the cyber and information risk incident management process:
   (a) Establishment of a designated team responsible for cyber and information security incident management.
   (b) Have sufficient capacity of qualified forensic staff who should be continuously trained or contracted team for handling major incidents.
   (c) A restricted area to facilitate the computer emergency response team workspaces.
   (d) Classification of cyber and information risk incidents.
   (e) Timely handling of cyber and information risk incidents, recording and monitoring progress.
   (f) Protection of relevant evidence and loggings.
   (g) Post-incident activities, such as forensics and root-cause analysis of the incidents.
   (h) Escalation of suggested improvements to the CISO and senior management.
   (i) Establishment of a cyber and information risk incident repository.
5. Inform the Bank of Zambia immediately a medium or highly classified cyber and information risk incident is discovered and before any media interaction related to the incident.
6. Submit a formal incident report to the Bank after investigations, which shall include root-cause analysis and corrective actions performed.

11.2 COMMUNICATIONS

The regulated entity shall:

1. Have a communication plan which includes a clear direction to ensure that only statements approved by senior management are released to relevant stakeholders.
2. Coordinate response activities with internal and external stakeholders consistent with the response and recovery plans.
3. Document and secure standard procedures for internal and external communications for use in an event of an incident.
4. Ensure employees know their roles and order of operations when a response and recovery process is needed.
5. Have consistency with respect to information shared with the response and recovery plans.
6. Share information with all relevant stakeholders to achieve broader cyber and information risk situational awareness.

11.3 ANALYSIS

The regulated entity shall:

1. Identify the threat scenarios that might have a potential impact on its business and determine which pieces of digital evidence shall be collected to facilitate forensic investigation.
2. Identify and document the digital evidence available on its systems and location and understand how the evidence shall be handled throughout its life cycle.

3. Develop procedures for securely collecting, handling, and storing digital evidence in a forensically acceptable manner, demonstrate that the evidence's integrity and authenticity is preserved and in accordance with the requirements defined in the policy, and appropriate laws and regulations.
4. Closely integrate plans for forensic readiness with plans for incident management and other related business planning activities.
5. Establish a management review process that improves forensic readiness plans in accordance with experience and new knowledge.
6. Collaborate with the relevant stakeholders to improve lawful forensic investigation and incident handling methodologies and tools.

11.4 MITIGATION AND IMPROVEMENT

The regulated entity shall:

1. Maintain a cyber and information risk incident response plan.
2. Respond to cyber and information risk incidents in accordance with the documented procedures.
3. Maintain an incident response plan that includes steps necessary to contain incidents.
4. Record/log and retain all incidents in line with relevant laws and regulations, and internal policy.
5. Mitigate and document newly identified vulnerabilities.
6. Review vulnerability reports and ensure all vulnerabilities are mitigated timely.
7. Closely integrate cyber and information risk incident response, resumption and recovery processes with crisis management, business continuity, and disaster recovery planning and operations.
8. Incorporate lessons learned in response plans.
9. Update response strategies.

PART VIII

12 RECOVER

This process involves the execution and maintenance of recovery processes and procedures to facilitate timely restoration of systems or assets affected by cyber and information risk events.

The Bank expects the regulated entity to undertake the following in recovering from cyber threats and attacks:

1. Put in place a recovery plan to enable operations in a diminished capacity and safely restore services.
2. Define recovery point objectives (RPOs) and its recovery time objectives (RTOs) commensurate with business needs and systemic role in the ecosystem.
3. Provide recovery teams with training the ability to respond to a disruptive event requiring cyber and information risk incident plan activation.
4. Ensure recovery team members understand the team's recovery goal, procedures to execute and how interdependencies between recovery teams may affect overall strategies.
5. Review a range of cyber and information risk scenarios and conduct the business impact analysis in line with the evolving threat landscape, on a regular basis.
6. Develop a recovery strategy based on the Business Impact Analysis (BIA).
7. Revise recovery planning processes by incorporating lessons learned.
8. Update recovery strategies regularly.
9. Manage public relations and communicate recovery activities to internal and external stakeholders.

PART IX

13 CYBERSECURITY MATURITY LEVEL ASSESSMENT

The regulated entity shall conduct a cyber and information security maturity assessment to ascertain its level of maturity. Such assessments shall be conducted annually commensurate with the size and complexity of the regulated entity. The methodology and tools used to perform the assessment together with the results shall be submitted to the Bank of Zambia.

PART X

14 AMENDMENTS

These Guidelines may be reviewed by the Bank as deemed necessary.

15 REVOCATION

Gazette notice number 333 of 2023 is hereby revoked.

16 EFFECTIVE DATE

These guidelines shall come into force on the date they are published in the Gazette.

Dated the 12th day of April 2023.

F. CHIPIMO,
Deputy Governor – Operations Bank of Zambia

LUSAKA