



GUIDANCE NOTE ON CYBERSECURITY

AUGUST 2026

GUIDANCE NOTE ON CYBERSECURITY

PART I Preliminary

- 1.1 Title
- 1.2 Authorization
- 1.3 Application
- 1.4 Definitions

PART II Statement of Policy

- 2.1 Purpose
- 2.2 Scope
- 2.3 Responsibility
- 2.4 Examples of Sources of Cyber Risk

PART III Specific Requirements

- 3.1 Governance
- 3.2 Cybersecurity Strategy and Policies
- 3.3 Risk Management Framework – Technology and Cybersecurity
- 3.4 Management of Technology Services
- 3.5 Technology Resilience
- 3.6 Access Rights and System Privileges
- 3.7 Data and Infrastructure Security
- 3.8 IT Service Management
- 3.9 Regular Independent Assessment and Test
 - 3.9.1 Role of Internal Auditors
 - 3.9.2 Role of Risk Management Function
 - 3.9.3 Role of External Auditors
- 3.10 Outsourcing
- 3.11 Training/Awareness

PART IV Reporting

ANNEXES

- I. High-level contents of a Cybersecurity policy
- II. Cybersecurity incident record template (*Immediate*)
- III. Cybersecurity incident record template (*Quarterly*)

PART I: PRELIMINARY

- 1.1 **Title** – Guidance Note on Cybersecurity.
- 1.2 **Authorization** - This Guidance Note is issued under Section 33(4) of the Banking Act, which empowers the Central Bank of Kenya (CBK) to issue Guidance Notes to be adhered to by institutions in order to maintain a stable and efficient banking system.
- 1.3 **Application** – This Guidance Note applies to all institutions licensed under the Banking Act (Cap. 488).
- 1.4 **Definitions** – The terms and acronyms used in this Guidance Note are defined below:
 - 1.4.1 **“BS-SOC”** means the Banking Sector Cybersecurity Operations Centre, established to coordinate sector-wide cybersecurity monitoring, detection, prevention, response, and recovery activities.
 - 1.4.2 **“Business Continuity”** is a state of continued and uninterrupted operation of a business.
 - 1.4.3 **“Business Continuity Management”** 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 minimize the operations, financial, legal, reputational and other material consequences arising from disruption.
 - 1.4.4 **“Business Continuity Plan”** 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 organization in the event of a disruption.
 - 1.4.5 **“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.
 - 1.4.6 **“Critical Information Infrastructure (CII)”** refers to interconnected information systems and networks, the disruption of which would have serious impact on the economic well-being of customers, or on the effective functioning of financial institutions and the economy.
 - 1.4.7 **“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

Technology (IT) systems and/or the internet and targeting the computers, IT infrastructure and internet presence of another entity.

- 1.4.8 “Cyber Assets”** are programmable electronic devices, communication networks, including hardware, software and data.
- 1.4.9 “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.
- 1.4.10 “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.
- 1.4.11 “Cybersecurity incident”** means an occurrence that-
- (a) jeopardizes without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
 - (b) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- 1.4.12 “Cyberspace”** is the virtual space created by interconnected computers and computer networks on the internet.
- 1.4.13 “IT Infrastructure”** refers to the hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and/or customers and is usually internal to an organization and deployed within owned facilities.
- 1.4.14 “Red Team Exercise”** refers to an all-out attempt to gain access to a system by any means necessary, and usually includes cyber penetration testing, physical breach, testing all phone lines for modem access, testing all wireless and systems present for potential wireless access, and also testing employees through several scripted social engineering and phishing tests. These are real life exercises carried out by an elite small team of trained professionals that are hired to test the physical, cybersecurity, and social defenses of particular systems.

PART II: STATEMENT OF POLICY

2.1 Purpose

This Guidance Note 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. Therefore, the purpose of this Guidance Note is to:

- Create a safer and more secure cyberspace that underpins information system security priorities and promotes stability of the Kenyan banking sector;
- Establish a coordinated approach to the prevention and combating of cybercrime;
- Up-scaling of identification and protection of critical information infrastructure;
- Promotion of compliance with appropriate technical and operational cybersecurity standards;
- Development of requisite skills, continuous building of capacity and promote a culture of fostering a strong interplay between policy, leveraging on technology to do business and risk management; and
- Maintenance of public trust and confidence in the financial system.
- Strengthen the capacity of the BS-SOC to monitor, detect, prevent, and respond to cyber threats within the banking sector, and to facilitate sector-wide coordination on incident reporting, capacity building, and technical response.

2.2 Scope

This Guidance Note sets the minimum standards that institutions should adopt to develop effective cybersecurity governance and risk management frameworks. It is not a replacement for and does not supersede the legislation, regulations and guidelines that institutions must comply with as part of their regulatory obligations, particularly in the areas of risk management, outsourcing, information communication technology, internal controls and corporate governance.

2.3 Responsibility

The board of directors and senior management of an institution are expected to formulate and implement Cybersecurity strategies, policies, procedures, guidelines and set minimum standards for an institution. All these must be documented and made available for review by external auditors and CBK.

2.4 Sources of Cybercrime

Cyber-attacks launched against information systems have placed the abuse of cyberspace high in the domestic as well as international agenda. Some illustrations of cybercrime activities include: -

- A breach in institutions' databases exposing data to cyber criminals.

- 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.
- People-related attacks like phishing, malware introduction through social engineering that can be utilized to gain privileged system access to critical systems.
- Interconnectedness of institutions could lead to compromise in the institutions' entry points, such as through service providers.
- Internal IT 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.
- Weak authentication controls for customer data, transactions and systems.

PART III: SPECIFIC REQUIREMENTS

3.1 Governance

a) Board of Directors

All board members need to have a deep understanding of their institution's core business operations and the evolving landscape of cyber threats involved. Robust oversight and engagement on cyber risk matters at the board level promotes a security risk-conscious culture within the institution. The board's responsibilities in relation to cyber risk include:

- i. Oversee the cultivation and promotion of an ethical governance, management culture and awareness. Setting "the right tone from the top" is a crucial element in fostering a robust cyber risk management culture.
- ii. Engage management in establishing the institution's vision, risk appetite and overall strategic direction with regard to cybersecurity.
- iii. Ensure the allocation of adequate cybersecurity budget based on the institution's size, complexity, and risk profile.
- iv. Assess management's evaluation of the institution's cybersecurity preparedness relative to its cyber risk exposure. This includes the adoption of an effective internal cybersecurity control framework with submission of periodic independent reports. Institutions should determine the scope and frequency of independent reports. However, comprehensive independent reports from internal and external audits should be performed continuously and on an annual basis, respectively.
- v. Define and periodically review cybersecurity risk ownership and management accountability, assigning clear responsibilities to relevant stakeholders; the coverage should include relevant business lines and not just the IT function.

- vi. Approve and regularly review the cybersecurity strategy, governance charter, policies and frameworks. These documents should clearly articulate how cyber risks are identified, managed, and mitigated in a comprehensive, integrated manner, tailored to the institution's unique risk profile, operational scale, and business nature.
- vii. Ensure that the cybersecurity policies are uniformly applied across all of the bank's operating entities, including subsidiaries, joint ventures and geographic regions.
- viii. Review on a regular basis the implementation of the institution's cybersecurity framework and implementation plan, including the adequacy of existing mitigating controls. The review should be done at least once in 12 months.
- ix. Incorporate cybersecurity as a standard agenda item in Board meetings to maintain awareness and responsiveness.
- x. Evaluate the results of management's ongoing monitoring efforts regarding the institution's cyber threat exposure and preparedness, ensuring proactive risk management.
- xi. Ensure the cybersecurity policy incorporates comprehensive monitoring metrics supported by detailed reporting and trend analysis, to facilitate informed decision-making and timely interventions.
- xii. Review and approve the institution's cyber risk assessment and business impact analysis (BIA) annually.

b) Senior Management

Senior Management of an institution holds ultimate responsibility for translating and implementing the institution's business strategy, risk appetite and threat landscape into actionable measures. Accordingly, the Senior Management should: -

- i. Implement the board-approved cybersecurity strategy, policies, and frameworks, ensuring alignment with the institution's overall business objectives.
- ii. Identify critical business processes, assets, and potential cyber threats, while maintaining a clear view of the institution's cyber risk exposure.
- iii. Ensure the creation of mitigation and recovery procedures to contain cyber risk incidents, reduce losses and return operations to normal. However, it is worth noting that an institution is also required to have in place Business Continuity Management (BCM) processes for the entire institution, as cyber risk is managed within the context of overall IT risk management.
- iv. Continuously improve the collection, analysis, and reporting of cybercrime information. This can be achieved through understanding the business environment institutions operate in, potential cyber risk points and referring to international best practices.

- v. Oversee the deployment of strong authentication mechanisms to safeguard customer data, transactions and institutional systems.
- vi. Ensure the provision of a sufficient number of skilled staff for the management of cybersecurity, who should be subjected to enhanced background and competency checks. Ensure timely and regular reporting to the board on the cyber risk status of the institution.
- vii. Establish a cybersecurity benchmarking framework with the Board's endorsement, to measure and compare cybersecurity performance against industry standards.
- viii. Incorporate cybersecurity as a standard agenda item in Senior Management meetings to reinforce its strategic importance.
- ix. Provide regular reports of the institution's cybersecurity posture to the board.
- x. 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;
 - Incident detection and assessment, reporting; and
 - Escalation and strategies deployed.
- xi. Collaborate with other institutions and security agencies to share the latest cyber threats/attacks encountered by the institution.
- xii. Create a post-incident analysis framework to determine corrective actions to prevent similar incidents in the future.
- xiii. 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 where necessary.
- xiv. Establish a formal operational linkage with the BS-SOC for real-time threat intelligence sharing, incident reporting, and coordinated responses.
- xv. Designate a BS-SOC Liaison Officer within senior management responsible for sector-level coordination, cyber threat intelligence exchange, and submission of incident or vulnerability reports to BS-SOC.
- xvi. Define procedures for joint incident management with BS-SOC during major events that may impact sectoral stability.

c) Chief Information Security Officer (CISO)

As cyber-attacks evolve, subjecting institutions to threats such as information theft, CBK expects the leadership of institutions to ensure strategic means are incorporated so as to enable a proactive approach to cybersecurity. One of the strategic measures globally accepted and acknowledged by CBK has been the introduction of the role of the Chief Information Security Officer (CISO). This role is aimed at creating an organizational culture of shared cybersecurity ownership.

Each institution should determine the best reporting option of the CISO depending on factors such as an institution's 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. Consequently, the CISO could report to the either the Chief Executive Officer (CEO), Chief Information Officer, Chief Operating Officer or Risk Function. Most importantly is to ensure that the CISO serves in the Senior Management Team.

The CISO is responsible for:

- i. Overseeing and implementing the institution's cybersecurity program and enforcing the cybersecurity policy.
- ii. 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.
- iii. 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.
- iv. 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).
- v. Organizing professional cyber related trainings to improve technical proficiency of staff.
- vi. Ensure that regular and comprehensive cyber risk assessments are conducted.
- vii. Ensure that adequate processes are in place for monitoring IT systems to detect cybersecurity events and incidents in a timely manner.
- viii. Reporting to the Board and Senior Management 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.
- ix. Ensure timely update of the incident response mechanism and Business Continuity Plan (BCP) based on the latest cyber threat intelligence gathered.

- x. Incorporate the utilization of scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.
- xi. Ensure frequent data backups of critical IT systems (e.g. real time back up of changes made to critical data) are carried out to a separate storage location.
- xii. 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.
- xiii. 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.
- xiv. Include BS-SOC in the institution's escalation matrix for all significant cybersecurity incidents affecting service delivery or sector critical infrastructure.
- xv. Facilitate the timely exchange of cyber threat intelligence with BS-SOC, under CBK's coordination, ensuring confidentiality and regulatory compliance.
- xvi. Coordinate with BS-SOC to participate in sector-wide cyber-drills, simulations, and red-team exercises to test resilience and incident readiness.

3.2 Cybersecurity Strategy and Policies

To effectively safeguard its information assets, an institution should develop a comprehensive cybersecurity strategy and a supporting set of policies that clearly articulate how vulnerabilities, emerging threats, and other cyber risks will be managed.

3.2.1 Cybersecurity Strategy

The institution should have a formal enterprise-wide cybersecurity strategy that is aligned with its various business objectives, stakeholder expectations, and broader risk management framework. The strategy should reflect the institution's risk tolerance and appetite, and demonstrate how cybersecurity supports operational resilience and long-term sustainability.

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

At a minimum, the cybersecurity strategy should include:

- a) A clear statement of the importance of cybersecurity to the institution.
- b) High-level cybersecurity expectations and requirements from key stakeholders.
- c) The institution's cyber resilience vision, mission and objectives.

- d) The defined cyber risk appetite, as well as cyber resilience targets and implementation plan.
- e) The required resources and technology to effectively manage and implement cyber resilience initiatives.
- f) Integration of cybersecurity with business continuity and disaster recovery.
- g) The technology and security controls necessary to protect critical information assets.
- h) A framework for meeting regulatory compliance and obligations.
- i) A communication and stakeholder engagement plan for internal and external audiences.

3.2.2 Cybersecurity Policy

The institution should implement a Cybersecurity Policy that operationalizes its cybersecurity strategy. This policy should provide clear guidance on how the institution identifies, mitigates, monitors, and manages cyber risks in alignment with its objectives and enterprise risk management framework. At a minimum, the Cybersecurity Policy should:

- a) Outline how the institution sets its risk tolerance and cyber resilience objectives and state how the institution identifies, mitigates and manages its cyber risk to support its objectives.
- b) Provide guidance on cybersecurity governance, capability development, information sharing and third-party/vendor risk management.
- c) Incorporate monitoring metrics coupled with reporting and trend analysis:
 - Define procedures for real-time monitoring of cyber threats.
 - Establish reporting structures for security incidents and vulnerabilities.
 - Depending on the level of inherent risks, identify their riskiness as low, moderate, high and very high or adopt any other similar categorisation.
- d) Ensure alignment with the institution's enterprise risk management framework by:
 - Ensure cybersecurity is integrated into broader risk management processes.
 - Define escalation procedures for reporting cyber incidents to executive management, the board, regulators, customers and any other key and relevant stakeholders.

3.3 Risk Management Framework – Technology and Cybersecurity

a) Risk Management Framework

- i) An Institution should establish a comprehensive risk management framework to manage technology and cyber risks. Appropriate governance structures and processes should be established, with well-defined roles, responsibilities and clear reporting lines across the various organisational functions.
- ii) The framework should incorporate effective risk management practices and internal controls designed to safeguard data confidentiality, maintain data integrity, and ensure the security, reliability, stability, and resilience of the institution's IT operating environment.
- iii) Effective risk management practices and internal controls should be incorporated to achieve data confidentiality and integrity, system security and reliability, as well as stability and resilience in its IT operating environment.
- iv) A risk officer, who is accountable for ensuring proper risk treatment measures are implemented and enforced for specific technology and cyber risks, should be identified.

b) Components of the Technology and Cyber Risk Management Framework

1) Technology and Cyber Risk Identification

An institution should:

- i) Establish a structured process to conduct regular Vulnerability Assessment (VA) on their IT systems to identify security vulnerabilities and ensure risks arising from these gaps are remediated in a timely manner.
- ii) Identify any threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third-party service providers.
- iii) Perform a VA which should at a minimum include vulnerability discovery, identification of weak security configurations and open network ports as well as application vulnerabilities. For web-based systems, the scope of VA should include checks on common web-based vulnerabilities.

2) Technology and Cyber Risk Penetration Testing (PT)

- i) Institutions should establish a process to conduct regular vulnerability assessment (VA) and Penetration Testing (PT) on their IT systems to identify security vulnerabilities and ensure risk arising from these gaps are addressed in a timely manner. The frequency of

VA and PT should be commensurate with the criticality of the IT system and the security risk to which it is exposed.

3) Technology and Cyber Risk Assessment

- i) An Institution should perform an analysis of the potential impact and consequences of the threats and vulnerabilities on the overall business and operations. When assessing technology and cyber risks, consideration should be given to financial, operational, legal, reputational, and regulatory factors.
- ii) To facilitate the prioritisation of technology risks, institutions should establish clear criteria for measuring the likelihood an impact of different risk scenarios. This enables a structured approach to risk ranking and resource allocation.

4) Technology and Cyber Threat Exercise

- i) Institutions should undertake regular scenario-based technology and cyber threat exercises to validate their response and recovery capabilities to prevalent and emerging threats. These exercises can include social engineering, table-top or cyber range exercises.
- ii) An Institution should design the exercise scenario by using threat intelligence relevant to their IT environment to identify threat actors who are most likely to pose a threat to them and identify tactics, techniques and procedures most likely to be used in such attacks.

5) Technology and Cyber Risk Remediation Management

- i) A comprehensive remediation process should be established to track and resolve issues identified from the technology and cybersecurity assessments or exercises. The process should minimally include the following:
 - Severity assessment and classification of an issue
 - Timeframe to remediate issues of different severity; and
 - Risk assessment and mitigation strategies to manage deviation from the framework.
- ii) A technology and cyber incident response and management plan should be established to swiftly isolate and neutralise the threat and securely resume affected services.

- iii) Information from cyber intelligence and lessons learnt from the technology and cyber incidents should be used to enhance the existing controls or improve the technology and cyber incident management plan.
- iv) An Institution should develop and implement risk mitigation and control measures that are consistent with the criticality of the information assets and the level of risk tolerance.
- v) Institutions should obtain insurance coverage for various insurable technology and potential cyber risks to reduce the financial impact such as recovery and restitution costs.

6) Technology and Cyber Risk Monitoring, Review and Reporting

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

- a) Establish a security operations centre (SOC) or engage managed security services.
- b) Establish a process to collect, process, review and retain system logs to facilitate its security monitoring operations. The logs should be protected against unauthorised access.
- c) Facilitate the identification of anomalies by establishing a baseline profile of each IT system's routine activities and analysing the system activities against the baseline profiles. The profiles should be regularly reviewed and updated.
- d) Ensure timely escalation of suspicious or anomalous system activities or user behaviours to relevant stakeholders.
- e) Maintain a risk register to facilitate the monitoring and reporting of technology and cyber risks. Significant risks should be monitored closely and reported to the board of directors and senior management. The frequency of monitoring and reporting should be correspondent with the severity of risk.
- f) Develop technology risk metrics to highlight information assets that have the highest risk exposure to facilitate risk reporting to management. In determining the technology

3.4 Management of Technology Services

a) Project Management Framework

Institutions should establish a comprehensive project management framework to ensure consistency, accountability, and successful delivery of IT initiatives. The framework should ensure:

- a) Consistency in project management practices, and delivery of outcomes that meet project objectives and requirements.
- b) Policies, standards, procedures, processes, and activities are included to guide the management of projects from initiation to closure.
- c) Detailed IT project plans are established for all IT projects. An IT project plan should set out the scope of the project, as well as the activities, milestones and deliverables to be realised at each phase of the project. The roles and responsibilities of staff involved in the project should be clearly defined in the plan.
- d) A risk management process is established to identify, assess, treat and monitor the associated risks throughout the project life cycle.

A project committee consisting of key stakeholders should be formed to provide guidance and oversight for large and complex projects that impact the operations of the business. This is to ensure milestones are reached and deliverables are realised in a timely manner.

b) System Development Life Cycle (SDLC)

- In order to minimise system vulnerabilities, security should be incorporated within each phase of the SDLC. An Institution should include security specifications in the system design, perform continuous security evaluation and adhere to security practices throughout the SDLC.
- Security requirements should minimally cover key control areas such as access control, authentication, authorisation, data integrity and confidentiality, system activity logging, security event tracking and exception handling.

c) Vendor Evaluation and Selection

- Institutions should establish standards and procedures for vendor evaluation and selection to ensure the selected vendor is qualified and able to meet its project requirements and deliverables. The level of assessment and due diligence performed should be commensurate with the criticality of the project deliverables.

3.5 Technology Resilience

a) Data Centre Resilience

Institutions should design and operate data centres with high resilience and redundancy to ensure continuity of critical business operations. The following are some of the key considerations:

- An institution should ensure data centres have redundant capacity components and multiple distribution paths serving the computer equipment to eliminate any single point of failure for effective achievement of the identified business recovery objectives.
- An institution shall host critical systems in a dedicated space intended for production data centre usage. The dedicated space must be physically secured from unauthorised access and is not located in a disaster-prone area.
- There should be no single point of failure in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure.
- Institutions should conduct adequate maintenance, and holistic and continuous monitoring of these critical components with timely alerts on faults and indicators of potential issues.

b) System Availability

- An institution should ensure that their IT systems are designed and maintained to achieve the level of system availability that is proportionate to its operational needs.
- Institutions to conduct regular system reviews and testing to ensure a robust level of resilience exists to facilitate sustainable business operations. At a minimum, the review should include a comprehensive mapping of internal and external dependencies of the institution's IT systems to identify potential single points of failure and evaluate the impact of their disruption on business operations.
- Institutions should implement effective monitoring mechanisms to track capacity utilisation, system performance, and the health of critical processes and services. These mechanisms must be capable of generating timely, actionable alerts that enable administrators to detect, investigate, and remedy service interruptions promptly. Monitoring parameters, including scope, metrics, and threshold values should be reviewed and updated periodically to ensure continued effectiveness and relevance.

c) System Backup and Restoration

- An institution should establish a robust backup and restoration strategy and procedures to meet business recovery objectives. They should support business continuity objectives, including the defined recovery time and recovery point requirements.
- At a minimum, an institution should-

- a) Establish backup and restoration procedures to effectively manage the backup data life cycle, including data classification, backup scheduling, retention, storage, retrieval, and secure disposal.
- b) Maintain an adequate number of backup copies of all critical data.
- c) Backup media must be stored in an environmentally secure and access-controlled facilities or backup sites that meet organisational and regulatory standards for physical and information security.
- d) Conduct periodic testing of backup and restoration procedures to validate recovery capabilities and alignment with business continuity objectives. Any failed test should trigger prompt root-cause analysis and timely remediation to prevent recurrence.
- e) Undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate, effective, and capable of safeguarding sensitive or mission-critical data throughout its life cycle.

3.6 Access Rights and System Privileges

- A financial institution should implement a comprehensive access control policy governing the identification, authentication, and authorisation of all users to its IT assets and data. The policy should define an appropriate level of granularity that reflects the institution's risk exposure to unauthorized access, data misuse, or compromise of system integrity.
- An institution shall adhere to the following principles:
 - a) Adopt a “deny all” access control policy for users by default, ensuring that all access to IT assets are explicitly authorized.
 - b) Employ “least privilege principle” access rights to ensure IT assets are accessed on a “need-to-have” basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles.
 - c) Establish a user access management process for provisioning, modifying and revoking user access rights to information assets. Access rights should be authorised and approved by appropriate parties, such as the information asset owner.
 - d) Where applicable, access privileges should be assigned for a defined duration based on the nature of the task or assignment, with automatic expiry upon completion.
 - e) All user access activities, including provisioning, modification, and termination, should be uniquely identified, logged, and retained to support auditability, investigations, and compliance requirements.
 - f) Institutions should define criteria for activities that require dual authorization control or four-eyes approval, especially for high-risk or sensitive activities.

- g) Ensure appropriate parties such as information asset owners or designated personnel conduct periodic user access reviews to verify the appropriateness of privileges that are granted to users. The user access review should be used to identify dormant and redundant user accounts, as well as inappropriate access rights. Exceptions noted from the user access review should be resolved as soon as practicable.
- Institutions should employ multi-factor authentication (MFA) for accessing critical systems, ensuring resilience against social engineering and credential-based attacks. The MFA mechanisms must incorporate at least two or more knowledge factors, inherent factors (e.g. biometric characteristics) or possession factors (e.g. security keys, tokens).
- An institution shall establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix must be periodically reviewed and updated.

3.7 Data and Infrastructure Security

3.7.1 Data Security

Institutions should establish and maintain comprehensive data protection and data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, exfiltration, or transmission of its confidential data, taking into consideration the following:

- a) data in motion - data that traverses internal networks, external networks or transmitted between geographically distributed sites;
- b) data at rest - data in endpoint devices such as notebooks, personal computers, portable storage devices and mobile devices, as well as data in systems such as files stored on servers, databases, backup media and storage platforms (e.g. cloud); and
- c) data in use - data that is being used or processed by applications or systems.

Institutions should implement appropriate and robust measures to prevent and detect and minimize the risk of data theft, leakage or unauthorised alteration within systems and endpoint devices. In addition, institutions should ensure that third-party managed service providers are accorded the same level of protection and are subjected to the same security standards.

3.7.2 Network Security

Institutions shall implement a defence-in-depth approach to securing their network infrastructure. At a minimum, the following controls should be implemented:

- a) Secure the network perimeter, including all external connections to the internet, as well as connections with third parties by installing network security devices such as firewalls, secure gateways, and network segmentation.
- b) Deploy effective security mechanisms to protect information assets to minimise the risk of cyber threats, such as insider-related threats.
- c) Detect and block malicious network traffic by deploying network intrusion detection and prevention systems in the network.
- d) Prevent unauthorised devices from connecting to its network by enforcing strict network access controls, device authentication.
- e) Review access control rules in network devices such as firewalls, routers, switches, and access points on a regular basis to ensure they are kept up to date. Promptly remove outdated rules, redundant configurations, and insecure network protocols as these can be exploited to gain unauthorised access to their network and systems.

3.8 IT Service Management

3.8.1 IT Service Management Framework

- Institutions should establish a robust IT service management framework to ensure effective delivery, monitoring, and continuous improvement of IT services. The framework should support operational stability, efficient incident response, structured change management, accurate tracking of information assets, and overall reliability of the production IT environment.
- At a minimum, the framework should define the governance structures, processes, and standard operating procedures for key IT service management disciplines, including configuration management, technology refresh management, patch management, change management, software release management, incident management and problem management.

3.8.2. Configuration Management

- Institutions should implement a configuration management process to maintain accurate, complete, and current inventory of all their hardware and software components to have visibility and effective control of their IT systems. The institutions should review and verify the configuration information of their hardware and software on a regular basis to ensure it is accurate and up-to-date.

3.8.3. Technology Refresh Management

- Institutions should not use outdated and unsupported hardware or software, which could increase their exposure to security and stability risks. The institution should closely monitor the hardware's or software's end-of-support (EOS) and end-of-life (EOL) timelines and develop a proactive technology refresh plan for the replacement of hardware and software before they reach EOS or EOL.
- A risk assessment should be conducted for all hardware and software approaching EOS or EOL to evaluate the risks associated with their continued use, and define effective risk mitigation measures or replacement strategies.

3.8.4 Patch Management

- Institutions shall establish a structured and timely patch management process to ensure applicable functional and non-functional patches (fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with the criticality of the patches and the institution's IT systems.
- All patches should be tested in a controlled, non-production environment before they are applied to the IT systems in the production environment. This is to ensure compatibility with existing IT systems and that they do not introduce new vulnerabilities or operational disruptions to the IT environment.

3.8.5 Change Management

- Institutions should establish a change management process to ensure changes to information assets are properly assessed, tested, reviewed and approved before implementation.
- A risk and impact analysis of the change to an information asset should be conducted before implementing the change. The analysis should cover security and implications of the change in relation to other information assets.
- All changes should be adequately tested in a designated test environment. Test plans for changes should be developed and approved by the relevant business and IT management. Test results should be formally accepted and signed off before the changes are deployed to the production environment.
- A change advisory board, comprising key stakeholders including business and IT management, should be formed to approve and prioritize the changes after considering the stability and security implications of the changes to the production environment.

- Institutions should perform appropriate backups of information assets prior to implementing any change and define a rollback plan to revert the information assets to their previous states if a problem arises during or after the change implementation.

3.8.6 Incident and Problem Management

- The occurrence of IT incidents such as system malfunctions, system errors, service interruptions, or network failures can disrupt operations and impact service delivery. Institutions should implement structured incident management procedures to ensure timely detection, escalation, containment, and resolution of such events.
- Root cause analysis should be conducted for significant or recurring incidents to prevent re-occurrence and strengthen system resilience.
- Problem management processes should complement incident management by identifying underlying structural issues, implementing corrective actions, and establishing preventative measure to minimise prolonged disruptions and mitigate future risks.

3.9 Regular Independent Assessment and Test

The understanding of the cyber threat landscape within institutions requires a collaborative approach that encompasses the following functions: Internal Audit, Risk Management and External Audit. 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 to evaluate their detection, prevention, and response posture.

- **Role of Internal Auditors**

All institutions must ensure that their Internal Audit function includes qualified Information and Communication Technology (ICT) Auditors. ICT Auditors can be outsourced or engaged on permanent employment. The institution's internal ICT auditors should then ensure that the audit scope includes and is not limited to the tasks below:

- i. Continuously review and report on cyber risks and the effectiveness of controls of the ICT systems within the institutions ICT environment and other related third-party integrations.
- ii. Assess both the design and operational effectiveness of the institution's implemented cybersecurity framework, including governance, policies, and technical controls.

- iii. Conduct regular independent threat and vulnerability assessments, including scanning and analysis of weaknesses across systems, networks, and applications.
- iv. Promptly report the findings of the assessments to the board or its relevant committee.
- v. Conduct comprehensive penetration tests to validate the institution's resilience against real-world attack scenarios.

- **Role of Risk Management Function**

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 a 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). The institution's risk management function should include and is not limited to the tasks below:

- i. Assessing cybersecurity risks and exposures ensuring they remain within the institution's defined risk appetite and tolerance levels.
- ii. Monitoring current and emerging risks, changes to laws and regulations, and industry developments that may impact the institution's risk posture.
- iii. Collaborating with system administrators and others charged with safeguarding the information assets of the institution to ensure appropriate control design and implementation.
- iv. Maintain comprehensive cyber risk registers: Key cybersecurity risks should be regularly identified, assessed and updated. Risk identification should be forward-looking and include security incident handling considerations.
- v. Ensure implementation of the cyber and information risk management strategy.
- vi. Ensuring protection of the confidentiality, integrity and availability of information across all business units and systems.
- vii. Ensure that a comprehensive inventory of IT assets, classified by business criticality, is established and maintained. A Business Impact Analysis process is in place to regularly assess the business criticality of IT assets.
- viii. Quantify the potential impact of the residual cyber risk by assessing and considering risks that could be addressed through cyber-insurance or risk transfer.
- ix. 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.
- x. Conduct red team exercises to simulate advanced adversary behaviour and assess detection and response capabilities.

- xii. The risk management function shall integrate BS-SOC threat advisories, alerts, and intelligence feeds into its cyber risk register and residual risk evaluation.

- **Role of External Auditors**

External auditors should incorporate IT and cybersecurity risk considerations into their annual audit scope. The scope should include and is not limited to:

- i. Understanding the institution's IT infrastructure, use of IT, operations and the impact of IT on financial reporting processes and related controls.
- ii. Assessing the extent of the institution's automated controls as they relate to financial reporting. This should include an understanding of the:
 - IT general controls that underpin systems supporting financial reporting.
 - Integrity and reliability of system-generated data and reports used in the audit.
- iii. Conduct independent threat and vulnerability assessments to evaluate security control maturity.
- iv. Comprehensive review of the adequacy and effectiveness of the approved cybersecurity strategies and policies.
- v. Conduct comprehensive penetration tests to independently validate the institution's exposure to cyber risks.
- vi. Report annually to the board and CBK on the key findings, weaknesses and recommendations for remediation based on the assessments conducted.

3.10 Third Party Technology Service Providers

As institutions expand their reliance on third party technology service arrangements, including cloud services and other external technology service providers, they face heightened cyber, operational, and compliance risks. Institutions must therefore ensure that all third parties adhere to applicable regulatory requirements, contractual obligations, and industry best practices. At a minimum, institutions should:

- Have in place adequate governance over outsourcing agreements, including due diligence on prospective service providers, documented outsourcing agreements and adequate monitoring of service delivery.
- Consider all outsourcing agreements as critical infrastructure for regulation and protection for purposes of security of the banking sector and the economy at large.
- Select their vendors based on rigorous risk-based compliance and risk assessments, factoring in security posture, compliance record, resilience and financial stability.
- Ensure all computing resources and digital assets are properly secured including registrations, licensing, compliance and verification.

- Ensure all outsourcing contracts require service providers to comply with applicable legal and regulatory frameworks.
- Understand the inherent risk arising from each third party, including access, data processing, system interconnections, and technology architecture.
- Perform risk analytics on an institution's outsourcing portfolio to understand which service providers pose the most relative risk to an institution.
- Work collaboratively with third parties to mitigate risks that pose the most risk to the institution, including coordinated testing, incident response procedures, and control enhancements.
- Monitor contracted third parties cyber posture for changes in their business structure, including expansions, divestitures, breaches and emerging vulnerabilities that may alter their risk profile. Service Level Agreements should have robust provisions in relation to security, service availability, performance metrics reporting obligations and penalties.
- Develop exit management strategies and contingency plans to ensure continuity of critical services in the event of termination, failure, or disruption of the outsourcing arrangement.

3.11 Training/Awareness

- Institutions should implement comprehensive IT and cybersecurity awareness training programmes designed to provide information on good IT security practices, common cyber threat vectors, emerging risks, and the institution's policies and procedures. The training should be provided for all employees including senior management and the board to ensure organization-wide cyber risk consciousness.
- A formalized, structured training plan should be established to provide ongoing technical training for cybersecurity professionals within the institution. This can include specialized training, certification pathways, hands-on exercises, and exposure to modern security tools and threat-hunting methodologies.
- Cybersecurity awareness and information should be extended to the institution's customers, clients, suppliers, partners, outsourced service providers and other third parties who have connectivity to the bank's IT infrastructure. This communication may include awareness communications, secure-usage guidelines, fraud prevention education, and advisory alerts on emerging threats.
- The training programme should be reviewed periodically to ensure its contents remain relevant, current and responsive to the evolving threat landscape. The review should take into consideration changes in the institution's IT security policies, prevalent and emerging risks, regulatory developments, and lessons learned from recent security incidents.

PART IV: REPORTING

- a) Institutions should notify the Central Bank of Kenya within 24 hours of any Cybersecurity and technology 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 in the format set out as **Annex II (Immediate)** to this Guideline. After an incident is resolved, institutions should submit a report indicating the cause, origin (internal or third party), remedial actions, lessons learned and supporting documentation (investigation reports or technical logs).
- c) On a quarterly basis, institutions shall provide Central Bank of Kenya with a report in the format set out as **Annex III (Quarterly)** to this Guideline, concerning its occurrence and handling of Cybersecurity and technology incidents via the email address:
fin@centralbank.go.ke.

In the event of any query or clarification, please contact:

The Director,
Bank Supervision Department
Central Bank of Kenya
P. O. Box 60000 - 00200,
Nairobi
Tel : 2860000
Email: fin@centralbank.go.ke

ANNEX I

HIGH LEVEL CONTENTS OF A CYBERSECURITY POLICY

The Cybersecurity Policy should generally include, at a minimum, the following components:

- **Governance:** Clear governance mechanisms outlining how the institution establishes, implements, monitors, and reviews its approach to cyber-risk management. This includes roles, responsibilities, escalation paths, and oversight structures.
- **Identification:** Processes for identifying critical business functions and the supporting information assets whose compromise could adversely affect financial stability, operational continuity, or customer trust. The policy should guide the classification and prioritization of these assets.
- **Protection:** Controls and measures designed to protect the confidentiality, integrity, and availability of the institution's systems, data, and services. This includes preventive security mechanisms, hardening standards, access controls, and defensive tooling.
- **Detection:** Capabilities enabling timely detection of anomalous activity or events that may indicate a cyber incident. Strong detection capabilities provide institutions with early warning signals to activate countermeasures and containment strategies.
- **Resumption:** Guidance on how the institution will contain, respond to, resume, and recover from cyber-attacks. This includes incident response playbooks, communication protocols, recovery timelines, and post-incident review processes.
- **Testing:** Requirements for rigorous testing of cybersecurity controls, systems and resilience mechanisms to validate their effectiveness. Testing may include penetration testing, vulnerability assessments, scenario exercises, and red-team engagements.
- **Situational awareness:** Processes for maintaining awareness of emerging threats, global cyber events, regulatory updates, and intelligence insights. Strong situational awareness enhances proactive risk management and speeds up detection, response, and recovery.
- **Learning and evolving:** Expectations for continuous improvement of cyber resilience. Financial institutions should cultivate a culture of cyber-risk awareness and adapt their cybersecurity frameworks in line with evolving technologies, risks, attack patterns, and lessons learned.
- **Collaboration:** Effective cyber resilience often requires coordinated efforts among financial institutions, industry partners, regulators, and threat-intelligence communities. Collaborative approaches can strengthen sector-wide defenses and accelerate response.
- **Organization and Resources:** Provision for adequate resourcing, including budget, tools, technologies, and skilled personnel to support cybersecurity activities. Allocations should align with the institution's risk profile and operational scale.

- **Cybersecurity Incident Management:** Requirements for a formalized cybersecurity incident response plan that outlines procedures, roles, communication flows, and tools to be used before, during, and after an incident.

ANNEX II

Cybersecurity/Technology Incident Record (*Immediate*)

[Insert Name of reporting financial institution]

[Insert Date and Time of reporting]: Date..... Time.....

Date of Incident	Time of Incident	Incident Status (Open, Resolved or Closed)	Nature of Incident (Chronological order of events)	Impact Assessment	Actions taken by the time of reporting

Submit the cybersecurity incident report within 24 hours after a cybersecurity incident(s) to the Bank Supervision Department at fin@centralbank.go.ke

Authorized Signatories

Signed for and behalf of

By the duly authorized Signatories

Name.....

Designation.....

Contact email.....

Contact phone number.....

Signature

Name

Designation

Contact email.....

Contact phone number.....

Signature

ANNEX III

Cybersecurity/Technology Incident Record (*Upon Resolution*)

[Insert Name of reporting financial institution]

[Insert Date and Time of reporting]: Date..... Time.....

Final Incident Report	
Date and time incident occurred:	
Date and time of resolution:	
Financial loss amount:	
Date and time of closure:	
Incident discovery method (how or via which channel was the incident discovered):	
Changes since the previous report (detailed chronological event, stakeholders notified):	
Impact assessment (financial loss amount, assessment on reputational impact based on customer complaints, description of systems affected as well as associated services):	
Incident description (Location, purpose of the system, name of service provider affected where applicable, affected applications /databases/ networks / storage / servers, etc.	
Incident closure (Indicate the root cause of the incident):	
Lessons and remediation:	

Submit the cybersecurity incident report within 24 hours after resolution of a cybersecurity incident(s) to the Bank Supervision Department at fin@centralbank.go.ke

Authorized Signatories

Signed for and behalf of

By the duly authorized Signatories

Name.....
Designation.....
Contact email.....
Contact phone number.....
Signature

Name
Designation
Contact email.....
Contact phone number.....
Signature

ANNEX IV

Cybersecurity/Technology Incident Record (*Quarterly*)

[Insert Name of participant]Quarter.....

No.	Date of Incident	Time of Incident	Nature of Incident	Action taken	Time of resolution	Action taken to mitigate future incidents
1.						
2.						
3.						
4.						
5.						

Submit this report on the 5th day after the end of every quarter to the Bank Supervision Department at fin@centralbank.go.ke

Authorized Signatories

Signed for and behalf of

By the duly authorized Signatories

Name.....

Designation.....

Signature

Name

Designation

Signature

REFERENCES

1. https://www.centralbank.go.ke/uploads/banking_sector_reports/452385077_Survey%20on%20the%20Adoption%20of%20the%202017%20CBK%20Guidance%20Cybersecurity%20to%20the%20Banking%20Sector.pdf
2. The 2024 Computer Misuse and Cybercrime (The Critical Information infrastructure and Cybercrime Management) Regulations: <https://nc4.go.ke/regulations/computer-misuse-cybercrime-cii-cybercrime-management-regulations-2024/>
3. <https://new.kenyalaw.org/akn/ke/act/2018/5/eng@2022-12-31>- Computer Misuse and Cybercrimes Act.
4. Central Bank of Malaysia – Risk Management in Technology, <https://www.bnm.gov.my/documents/20124/938039/pd-rmit-nov25.pdf>.
5. www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
6. <https://www.mas.gov.sg/regulation/forms-and-templates/incident-reporting-template>
7. <https://www.fsc.gov.bb/viewPDF/documents/2024-12-11-13-25-21-Technology--Cyber-Risk-Management-Guideline.pdf>
8. Bank of Mauritius – Guideline on Cyber and Technology Risk Management - https://www.bom.mu/sites/default/files/guideline_on_cyber_and_technology_risk_management.pdf
9. <https://www.bis.org/bcbs/publ/d454.pdf>
10. Reserve Bank of South Africa - <https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight/Directive%20in%20respect%20of%20cybersecurity%20and%20cyber-resilience%20within%20the%20national%20payment%20system.pdf>
11. <https://www.resbank.co.za/content/dam/sarb/publications/prudential-authority/pa-public-awareness/covid-19-response/2025/joint-comm3-of-2025/Joint%20Communication%203%20of%202025%20-%20Determinations%20notification%20-%20IT%20and%20cyber.pdf>
12. <https://www.fsb.org/2025/04/format-for-incident-reporting-exchange-fire-final-report/>