GUIDANCE NOTE ON CYBERSECURITY

AUGUST 2017

GUIDANCE NOTE ON CYBERSECURITY

PART I Preliminary

PART II Statement of Policy

PART III Specific Requirements

PART IV Reporting

ANNEXES

PART I: PRELIMINARY

1.1 Title – Guidance Note on Cybersecurity.

1.2 Authorisation - 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 '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.

1.4.2 '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 minimise 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 organisation in the event of a disruption.

1.4.5 '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.

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

1.4.7 '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.

1.4.8 '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.

1.4.9 'Cyberspace' is the virtual space created by interconnected computers and computer networks on the internet.

1.4.10 '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.

1.4.11 'Cyber Assets' are programmable electronic devices, communication networks including hardware, software and data.

1.4.12 'Cybersecurity incident' is any malicious act or suspicious event that: compromises, or attempts to compromise, the electronic security perimeter or physical security perimeter of a critical Cyber Asset or disrupts or attempts to disrupt, the operation of a critical Cyber Asset.

1.4.13 '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, cyber security, 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 promote 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.

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, policy, 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 introductions 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.
- Poor authentication controls to protect customer data, transactions and systems.

PART III: SPECIFIC REQUIREMENTS

3.1 Governance

a) Board of Directors

All board members should understand the nature of their institution's business and the 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 responsibilities of the board 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 regards to cybersecurity.
iii. Allocation of an adequate cybersecurity budget based on the institution's structure.
iv. Review management's determination of whether the institution's cybersecurity preparedness is aligned with its cyber risks. 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 audit should be performed continuously and on an annual basis respectively.

v. Establish or review cybersecurity risk ownership and management accountability and assign ownership and accountability to relevant stakeholders; the coverage should include relevant business lines and not just the IT function.
vi. Approve and continuously review the cybersecurity strategy, governance charter, policy and framework. The purpose of the cybersecurity strategy, policies and framework is to specify how to identify, manage, and mitigate cyber risks in a comprehensive and integrated manner. The strategy, policies and frameworks should be tailored based on the institution's risk profile, size, complexity and nature of their business processes.
vii. Ensure that the cybersecurity policy applies to 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 in Board meetings.
x. Review the results of management's ongoing monitoring of the institution's exposure to and preparedness for cyber threats.
xi. Ensure the cybersecurity policy incorporates monitoring metrics coupled with reporting and trend analysis.

b) Senior Management

Senior Management of an institution is responsible for implementing the institution's business strategy, risk appetite and threats. As such, the Senior Management should: -

i. Implement the board approved cybersecurity strategy, policy and framework.
ii. Understand cyber organizational scope as well as identify cyber threats, critical business processes and assets.
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 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 deployment of strong authentication measures to protect customer data, transactions and systems.
vi. Ensure the provision of 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.
viii. Incorporate cybersecurity as a standard agenda in Senior Management meetings.

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 the 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.

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

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.

3.2 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.

- **Role of Internal Auditors**

  All institutions to incorporate qualified Information and Communication Technology (ICT) Auditors within the Internal Audit team. ICT Auditors can be outsourced or 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 controls of the ICT systems within the institutions and other related third-party connections.
  ii. Assess both the design and effectiveness of the cybersecurity framework implemented.
  iii. Conduct regular independent threat and vulnerability assessment tests.
  iv. Report to the board the findings of the assessments.
  v. Conduct comprehensive penetration tests.

- **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 the duty to ensure that cybersecurity risks are managed within the enterprise risk management portfolio (as a dedicated category or as a subset of

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

i. Assessing the risks and exposures related to cybersecurity and determining whether they are aligned to the institution's risk appetite.
ii. Monitoring current and emerging risks and changes to laws and regulations.
iii. Collaborating with system administrators and others charged with safeguarding the information assets of the institution to ensure appropriate control design.
iv. Maintain comprehensive cyber risk registers: Key cybersecurity risks should be regularly identified and assessed. Risk identification should be forward looking and include the security incident handling.
v. Ensure implementation of the cyber and information risk management strategy.
vi. Safeguarding the confidentiality, integrity and availability of information.
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 by assessing the residual cyber risk and considering risks that need to be addressed through insurance as a way of transferring cyber risk.
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.

- **Role of External Auditors**

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

i. Obtaining an understanding of the institution's IT infrastructure, use of IT, operations and the impact of IT on financial reporting statements.
ii. Understanding the extent of the institution's automated controls as they relate to financial reporting. This should include an understanding of:
    - IT general controls that affect the automated controls.
    - Reliability of data and reports used in the audit that are produced by the institution.
iii. Conduct independent threat and vulnerability assessment.
iv. Comprehensive review of the approved cybersecurity strategy and policy.
v. Conduct comprehensive penetration tests.
vi. Report annually to the board and CBK on the findings of the assessments.

3.3 Outsourcing

Institutions are rapidly expanding their reliance on outsourcing, cloud providers and other services that are time saving and reduce operation costs. However, with this trend, risks such as cyber risk could also emanate. Institutions should therefore ensure that their third-parties comply with legal and regulatory frameworks as well as the international best practices. Generally, institutions should:

- Have in place adequate governance of 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 compliance and risk assessments.
- Ensure all computing resources are 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.
- Perform analytics on an institution's outsourcing portfolio to understand which pose the most relative risk to an institution.
- Work collaboratively with third parties to mitigate risks that pose the most risk to an institution.
- Monitor contracted third parties for changes in their business and cyber posture including expansions, divestitures, breaches and new attacks that may alter the third parties' exposure. Service Level Agreements should have robust provisions in relation to security, service availability, performance metrics or penalties.
- Develop exit management strategies and contingency plans.

3.4 Training/Awareness

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

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

- Cybersecurity awareness and information should be provided to the institution's customers, clients, suppliers, partners, outsourced service providers and other third parties who have links to the bank's IT infrastructure.

PART IV: REPORTING

a) CBK is well aware of the fact that cyber risk will keep morphing due to the evolution of cyber threats in Kenya and across the globe. Therefore, CBK mandates all institutions to review their cybersecurity strategy, policy, and framework regularly based on each institution's threat and vulnerability assessment. All institutions are required to submit their Cybersecurity Policy, strategies and frameworks to the Central Bank of Kenya by November 30, 2017. High level contents of a cybersecurity policy are outlined in **Annex I** to this Guidance Note.

b) The institutions should notify the Central Bank of Kenya within 24 hours of any Cybersecurity incident(s) that could have a significant and adverse impact on the institution's ability to provide

adequate services to its customers, its reputation or financial condition in the format set out as **Annex II (Immediate)** to this Guideline.

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 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 contain the following:

- **Governance:** Mechanisms put in place to establish, implement and review its approach to managing cyber risks.
- **Identification:** Operational failure can negatively impact financial stability hence the financial institutions are required to identify their critical business functions and supporting information assets so as safeguard them against compromise.
- **Protection:** Cyber resilience depends on effective security controls that protect the confidentiality, integrity and availability of its assets and services.
- **Detection:** Financial institution's ability to detect the occurrence of anomalies and events indicating a potential cyber incident is essential to strong cyber resilience. Early detection provides a financial institution with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches.
- **Resumption:** This relates to response and recovery and provides guidance on how a financial institution should respond in order to contain, resume and recover from successful cyber-attacks.
- **Testing:** Once employed within a financial institution, the elements of its cyber resilience framework should be rigorously tested to determine their overall effectiveness.
- **Situational awareness:** Strong situational awareness can significantly enhance a financial institution's ability to understand and pre-empt cyber events, and to effectively detect, respond to and recover from cyber-attacks that are not prevented.
- **Learning and evolving:** Financial institutions should aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the institution. There should be emphasis on importance of implementing an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks to enable effective management of those risks.
- **Collaboration:** Effective solutions may necessitate collaboration between financial institutions and their stakeholders as they seek to strengthen their own cyber resilience. Efforts to coordinate the design of resilience solutions may bring enhanced strategies forward, in a timelier and efficient way.
- **Organisation and Resources:** Allocation of an adequate cybersecurity budget based on the institution's structure and size of its cyber risk function.
- **Cybersecurity Incident Management:** Cybersecurity incident response plan should provide a roadmap for the actions the institution will take during and after a security incident.

ANNEX II

Cybersecurity Incident Record (*Immediate*)

[*Insert Name of participant*] ……...……

[*Insert Date and Time of reporting*]: *Date…… Time……*

Date of Incident	**Time of Incident**	**Nature of Incident (Chronological order of events)**	**Impact Assessment**

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

Signed for and behalf of ……
By the duly authorized Signatories

Name……...
Designation…….
Signature

Name …….
Designation ……
Signature

ANNEX III

Cybersecurity 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 10th day after the end of every quarter to the Bank Supervision Department at fin@centralbank.go.ke

Signed for and behalf of ……
By the duly authorized Signatories

Name……...
Designation…….
Signature

Name …….
Designation ……
Signature