DRAFT GUIDANCE NOTE ON CYBER RISK

JUNE 2017

GUIDANCE NOTE ON CYBER RISK

PART I Preliminary

PART II Statement of Policy

PART III Specific Requirements

PART IV Reporting

PART I: PRELIMINARY

1.1 Title – Guidance Note on Cyber Risk

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 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, 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, 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 fashion 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' 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 the event of a disruption.

1.4.5 'Cybersecurity': Cybersecurity in a nutshell can be defined as 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 of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.

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.

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, 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 Cyber Risk 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 hacker 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.
- Interconnectedness of institutions could lead to compromise in the institutions entry points such as through service providers.
- Internal IT systems can itself 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 and size of its cyber risk function.
iv. Review management's determination of whether the institution's cybersecurity preparedness is aligned with its cyber risks.
v. Adoption of an effective internal cybersecurity control framework with submission of periodic independent reports.
vi. Establish or review cyber security risk ownership and management accountability and assign ownership and accountability to relevant stakeholders; the coverage should include relevant business lines and not just the I.T function.
vii. 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.
viii. Ensure that the cyber security policy applies to all of the bank's operating entities, including subsidiaries, joint ventures and geographic regions.

ix. Review on a regular basis the implementation of the institution's cyber security framework and implementation plan, including the adequacy of existing mitigating controls.
x. Incorporate cyber security as a standard agenda in Board meetings.
xi. Review the results of management's ongoing monitoring of the institution's exposure to and preparedness for cyber threats.

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. Put in place adequate business resilience arrangements for disaster recovery and business continuity.
iv. Continuously improve collection, analysis, and reporting of cybercrime information.
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 cyber security, who should be subjected to enhanced background and security checks.
vii. Ensure timely and regular reporting to the board on the cyber risk status of the institution.
viii. Establish a cyber-security benchmarking framework with the Board's endorsement.
ix. Incorporate cyber security as a standard agenda in Senior Management meetings.
x. Provide regular reports of the institution's cybersecurity posture to the board.
xi. 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:

(a) the roles and responsibilities of staff;
(b) Incident detection and assessment, reporting; and
(c) Escalation and strategies deployed.

xii. Collaborate with other institutions and the security agencies to share the latest cyber threats/attacks encountered by the institution.

c) Chief Information Security Officer (CISO)

As cyber-attacks evolve placing institutions under 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 cyber risk ownership. 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 cyber security 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. Conducting regular and comprehensive cyber risk assessments that consider people (i.e. employees, customers, outsourcing and other external parties), processes, data, technology across all its business lines and locations.
vii. Monitoring current and emerging cyber risks.
viii. Maintain comprehensive cyber risk registers. Risk identification should be forward looking and include the security incident handling.
ix. Reporting to the board 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.
    - Cyber risk identification.
    - Assessment of the effectiveness of the approved cybersecurity program.
    - All material cybersecurity events that affected the institution during the period.
x. Ensure timely update of the incident response mechanism and Business Continuity Plan (BCP) based on the latest cyber threat intelligence gathered.
xi. Incorporate the utilization of scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.
xii. 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.
xiii. 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.
xiv. 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 cyber security expertise to assist in understanding their cyber threat landscape.

3.2.1 Roles of Internal Auditors

All institutions should incorporate qualified Information and Communication Technology (ICT) Auditors within the Internal Audit team. The institution's internal IT auditors should ensure that the audit scope includes and is not limited to the tasks below:

i. Continuously review the cyber risk and controls of the ICT systems within the institutions and other related third-party connections.
ii. Assess both the design and effectiveness of the cyber security framework implemented.
iii. Conduct regular independent threat and vulnerability assessment tests.
iv. Report to the board the findings of the assessments.

3.2.2 Roles 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 and the impact of IT on the financial 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 an independent threat and vulnerability assessment.
iv. Comprehensive review of the approved cybersecurity strategy and policy.
v. Conduct comprehensive penetration tests.
vi. Report to the board and CBK on the findings of the assessments.

3.3 Training/Awareness

- Institution's 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.
- A formalized plan should be put in place to provide ongoing technical training to cyber security specialists within the institution.
- Cyber security awareness and information should be provided to the institution's customers and clients as well.

PART IV: REPORTING

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 Cyber Security Policy, strategies and frameworks to the Central Bank of Kenya by 31st August 2017.

The institutions should also notify the Central Bank of Kenya immediately when it becomes aware of a cybersecurity incident 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 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