BANKI KUU YA KENYA

Central Bank of Kenya

Survey on the Adoption of the 2017 Central Bank of Kenya Guidance on Cybersecurity to the Banking Sector

Table of Contents

List of Figures

1.0 INTRODUCTION

- Technology-driven innovation and the digitalization of finance are changing both customer behaviors and the way that banking services are provided. New products, new entrants and the use of new technologies present both opportunities and risks for the banking ecosystem. It is, therefore, critical that banks implement a robust information and communication technology (ICT) framework, including cybersecurity and risk management, in alignment with their operational risk management framework and operational resilience approach.

- Accordingly, the Central Bank of Kenya (CBK) issued a Guidance on Cybersecurity (Guidance) to commercial banks in August 2017. The Guidance outlines the minimum requirements that institutions shall build upon in the development and implementation of strategies, policies, procedures and related activities aimed at mitigating cyber risk. In addition, the Guidance sets the minimum standards that institutions should adopt to develop effective cybersecurity governance and risk management frameworks.

- The survey was conducted to assess the level of cyber risk awareness, preparedness, and resilience within the financial sector following the issuance of the Guidance. This survey will help identify vulnerabilities, gauge the effectiveness of current security measures, and inform policy decisions to strengthen cyber defenses.

1.1 Survey Methodology

- The survey collected data from 37 commercial banks and 1 mortgage finance institution. The survey was issued in March 2025.

- Questions in the 2025 survey were classified into 9 sections:

  – **Section 1:** Governance.

  – **Section 2:** Regular Independent Assessment and Test.

  – **Section 3:** Outsourcing.

  – **Section 4:** Training and Awareness.

  – **Section 5:** Incident Response.

  – **Section 6:** Security Technologies.

  – **Section 7:** Impact and Challenges.

  – **Section 8:** Cybersecurity Maturity Assessment.

  – **Section 9:** General Comments.

2.0 SUMMARY OF FINDINGS

The key findings of the survey are:

- All commercial banks have a dedicated cybersecurity governance framework, cybersecurity policies, and a formalized business continuity management process in place. The policies are reviewed and updated regularly to align with industry's best practices, regulatory standards and emerging threats.

- Commercial banks indicated that they have budgeted between Ksh.19 million and Ksh.600 million towards cybersecurity indicating a growing awareness of the risks posed by sophisticated cyberattacks and a commitment to enhancing the security posture.

- 92 percent of commercial banks have Information Technology (IT) auditors within their internal audit teams, while 8 percent do not. Consequently, 97 percent of commercial banks conduct regular audits to evaluate the effectiveness of cybersecurity controls, while 3 percent do not.
- 95 percent of banks assess and manage cybersecurity risks posed by third-party vendors, while 5 percent do not. Institutions that did not assess and manage cybersecurity risks posed by third parties indicated that they vet their vendors before onboarding them.
- All commercial banks indicated that they provide regular cybersecurity awareness training for all employees.
- Commercial banks that adopted the 2017 CBK Cybersecurity Guidance agreed that it significantly:
  - Strengthened their cybersecurity governance and risk management.
  - Improved incident response capabilities and resilience.
  - Enhanced regulatory and compliance framework.
  - Improved cybersecurity resilience through initiatives such as setting up security operations center (SOC).
  - Increased capacity building and awareness on cybersecurity.
  - Improved security controls by implementing secure configuration baselines for IT systems.
  - Increased assurance on the systems and technical infrastructure supporting the banking sector.
- The respondents noted the following challenges that they faced concerning their endeavors to implement the Cybersecurity guidelines:
  - Risk management of Artificial Intelligence solutions.
  - Reliance on manual monitoring due to limited technology to provide real-time security visibility and monitoring to address emerging threats.
  - Continuous increase in the cost of cybersecurity maintenance.
  - Evolving cyber threat landscape.
  - High cost of technical training and tools.
  - High cost of attracting, retaining and motivating cybersecurity experts due to the shortage of cybersecurity experts.
- The respondents recommended the following emerging areas to be included in the Guidance:
  - Artificial Intelligence and machine learning.
  - Cloud computing and the corresponding governance framework.
  - Application programming interface security.
  - Cyber risk insurance and risk transfer mechanisms.
  - Enhanced controls on mobile money fraud detection.
  - Managing data protection related risks.
  - Threat intelligence sharing mechanism could be captured in the guidance note, once a framework has been developed to support anonymized intelligence sharing.

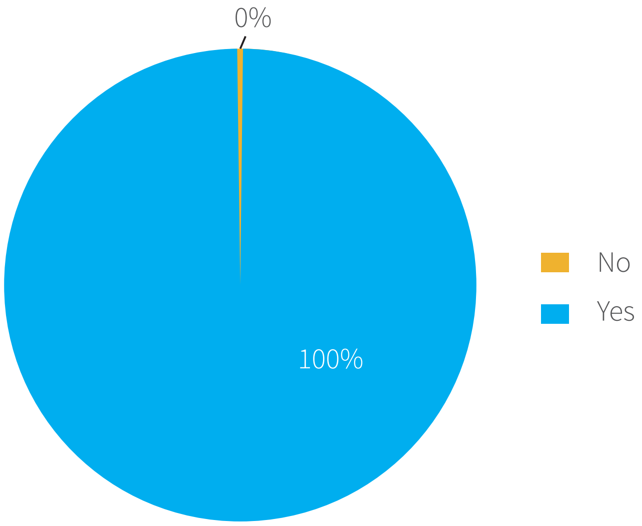
- Third-party cybersecurity guidelines and controls compliance.
- Regulatory framework for zero trust architecture.
- Digital identity.
- Internet of things security.

3.0 SURVEY FINDINGS

3.1 Governance

- 100 percent of the respondents indicated that they have a dedicated cybersecurity governance framework, cybersecurity policies, and a formalized business continuity management process in place. The policies are reviewed and updated regularly to align with industry's best practices, regulatory standards and emerging threats. In addition, the institutions indicated that senior executives and the board of directors are engaged in cybersecurity governance.
- 100 percent of the respondents have clearly defined and assigned roles and responsibilities regarding cybersecurity.

Figure 1: Institutions with a cybersecurity framework in place



- 95 percent of the respondents have a cybersecurity budget. Conversely, 5 percent indicated that they do not have a cybersecurity budget and that funds are availed when required. The cybersecurity budget is subsumed within the overall IT budget. Commercial banks indicated that they have budgeted between Ksh.2.5 million and Ksh.600 million annually towards cybersecurity indicating a growing awareness of the risks posed by sophisticated cyberattacks and a commitment to enhancing security posture. The budget was dependent on the cost of annual license fees of cybersecurity solutions implemented by the commercial banks.

- 82 percent of the respondents have stated that they have a Chief Information Security Officer (CISO). Out of the seven respondents without a CISO representing 18 percent, six plan on having a CISO in future. The CISO is responsible for protecting a bank's information and digital assets from cyber threats, ensuring compliance, and maintaining a strong security posture. A CISO's importance in a bank stems from the need to protect sensitive customer data, maintain operational stability, and uphold the bank's reputation and public trust.

- 100 percent of the respondents state that the cybersecurity team report regularly to the board of directors. This is essential for ensuring that cybersecurity is treated as a strategic business priority, not just a technical issue.

- 32 percent of the respondents stated that they conduct cyber risk assessments on a quarterly basis. 21 percent, 16 percent and 11 percent of the respondents stated that they conduct cyber risk assessments on an annual, monthly and semi-annual basis respectively. Cyber risk assessments in banking are a strategic necessity, not just a technical task. They support the protection of assets, ensure legal compliance, reduce financial exposure, and uphold customer trust in an increasingly digital financial ecosystem.

- 100 percent of the commercial banks state that cybersecurity risks are included in their organization's overall risk management framework. Majority of the respondents indicated that they have a process in place to monitor and adapt to changes in cybersecurity-related regulations.

  This is through the following:

  - o Information sharing through committees established by the Kenya Bankers Association (KBA).
  - o There is a regulatory department responsible for monitoring compliance requirements.
  - o The Audit, Risk, Compliance and Legal teams undertake periodic assessments of the respective units' compliance to the relevant regulations.
  - o Through peer information sharing.
  - o Through quarterly reporting where changes in cybersecurity related regulations are highlighted.
  - o Through industry workshops.

3.2 Regular Independent Assessment and Test

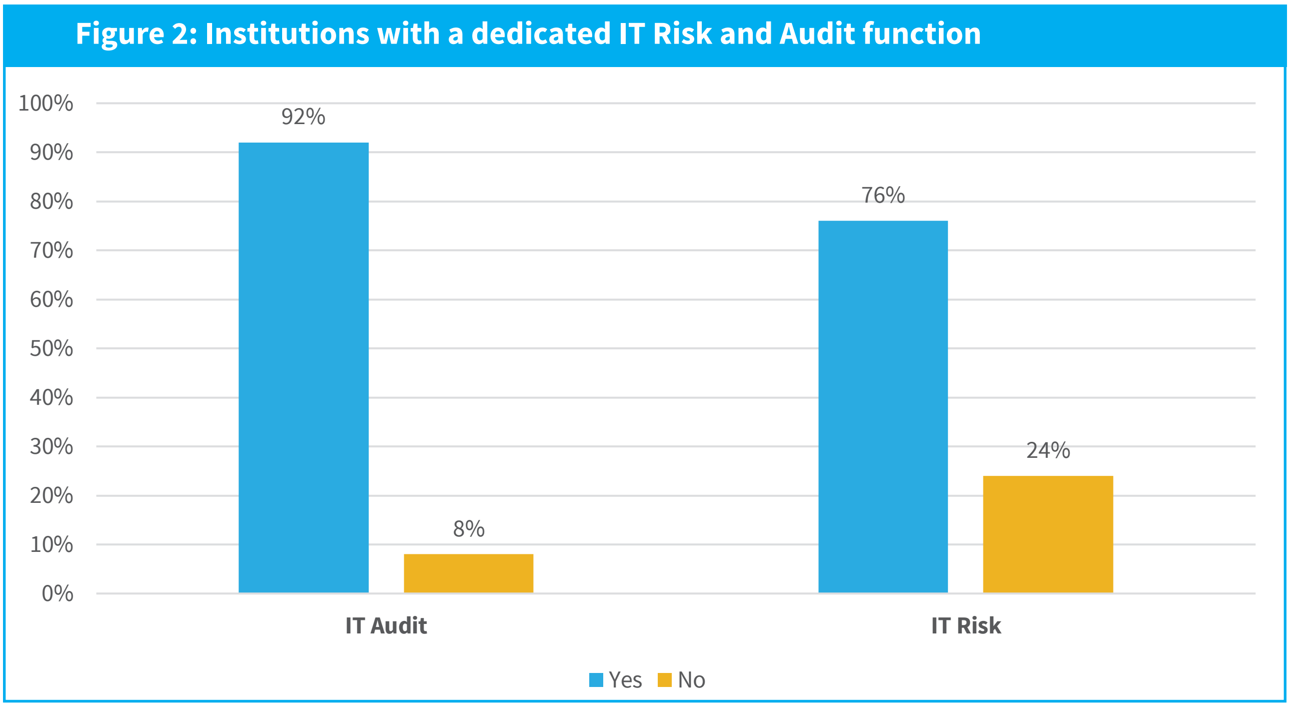
- The understanding of the cyber threat landscape within institutions requires a collaborative approach that encompasses the following functions: Internal Audit, Risk Management and External Audit.

- 92 percent of commercial banks have IT auditors within their internal audit teams, while 8 percent do not. Consequently, 97 percent of commercial banks conduct regular audits to evaluate the effectiveness of cybersecurity controls, while 3 percent do not.

- 76 percent of commercial banks have an IT risk function within their risk management structure, while 24 percent do not.

- The 2017 CBK Guidance on Cybersecurity requires commercial banks to conduct and report IT audits annually to the board. All commercial banks send their external IT audit reports to CBK annually.

Figure 2: Institutions with a dedicated IT Risk and Audit function

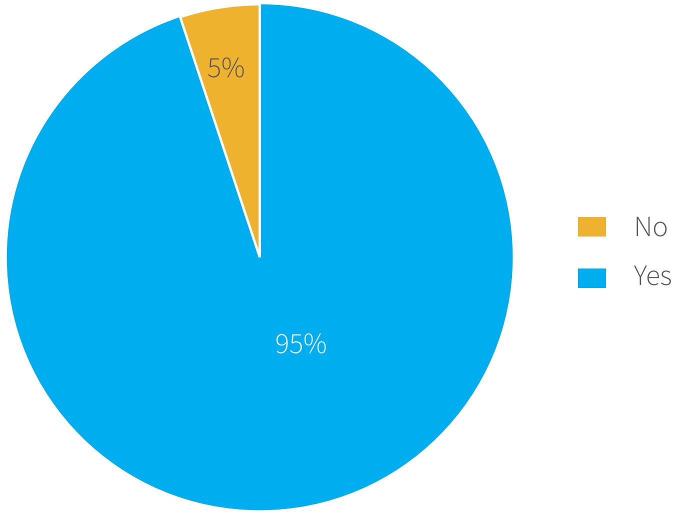


- All institutions (100 percent) indicated that they conduct vulnerability assessment and penetration testing on their systems, and cyber risk assessments on their systems either annually, quarterly or monthly. Vulnerability assessments assist institutions to identify potential weaknesses, while penetration tests simulate real-world attacks to exploit those weaknesses, providing a more realistic assessment of the security posture.

3.3 Outsourcing

- As the banking sector becomes increasingly interconnected and reliant on external partners, the risks associated with third-party vendors have become a significant vulnerability point for many banks.
- 95 percent of commercial banks assess and manage cybersecurity risks posed by third-party vendors, while 5 percent do not. Commercial banks that did not assess and manage cybersecurity risks posed by third parties indicated that they vet their vendors before onboarding them.

Figure 3: Institutions that assess and manage cybersecurity risks posed by third-party vendors



3.4 Training and Awareness

- All (100 percent) respondents indicated that they provide regular cybersecurity awareness training for all employees. This ensures that employees are well-equipped to identify and mitigate potential security threats. The training also keeps employees informed about emerging cyber threats, best practices for safeguarding sensitive information, and their roles in maintaining a secure work environment.

- 79 percent of commercial banks indicated that they monitored and enforced cybersecurity training for third-parties while 21 percent did not.

3.5 Incident Response

- 97 percent of respondents indicated that they have a cyber response plan in place. The plans are approved by management and cover the following areas:

  i) Roles and responsibilities of the incident response team.

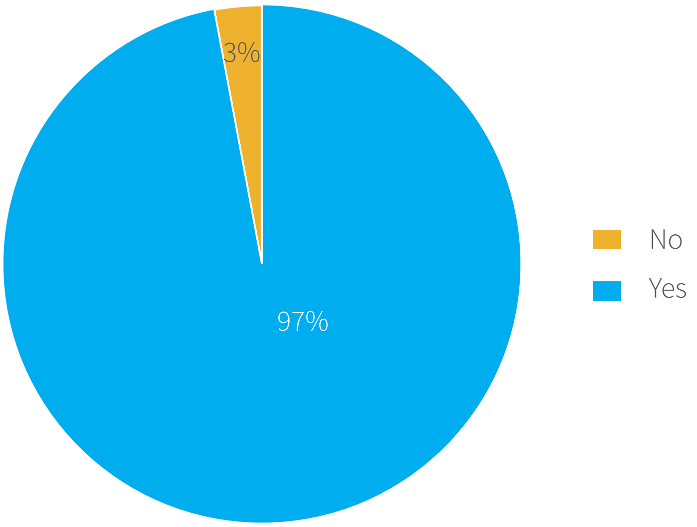
  ii) Incident detection and analysis.

  iii) Incident containment, eradication, and recovery.

  iv) Post incident analysis.

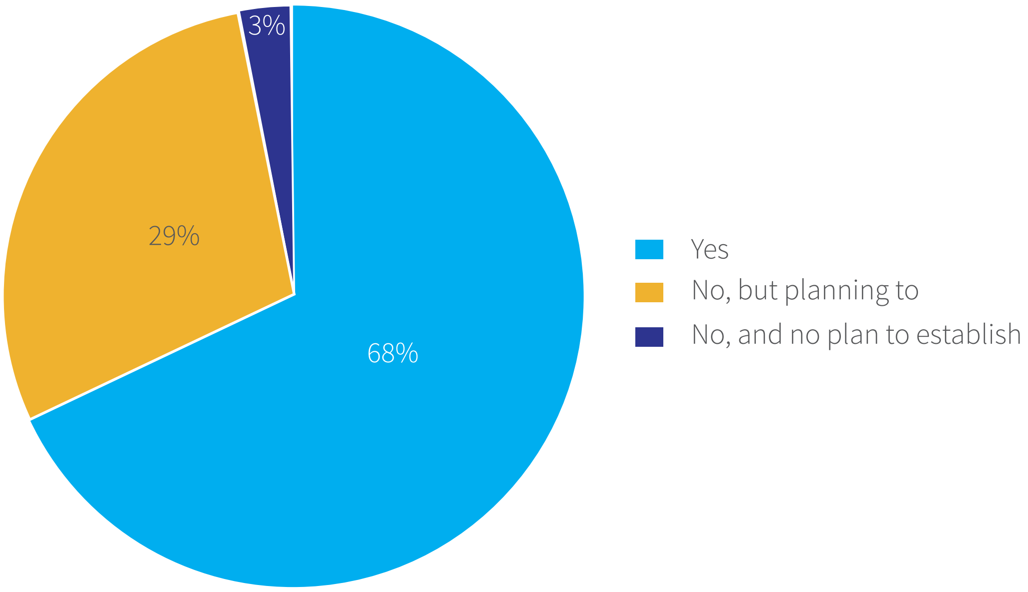
- Majority of the institutions noted that their incident response plans are reviewed and tested annually. The institution that did not have an incident response plan indicated that they are currently developing one.

Figure 4: Institutions with an incident response plan



- Of the commercial banks surveyed, 68 percent indicated that they had established a security operations center (SOC). 29 percent indicated that they did not have a SOC but were planning to set up one while 3 percent indicated that they did not have a SOC and were not planning to establish one. A SOC provides continuous monitoring, threat detection, and rapid response to cybersecurity incidents, ensuring that financial institutions stay ahead of potential threats.

Figure 5: Presence of a Security Operations Center



- 100 percent of the respondents indicated that they had a process for reporting cybersecurity incidents. In addition, all commercial banks indicated that key stakeholders are notified within defined timeframes during an incident. This is in line with the 2017 CBK Guidance on Cybersecurity which requires commercial banks to notify CBK within 24 hours of any cybersecurity incidents 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.

3.6 Security Technologies

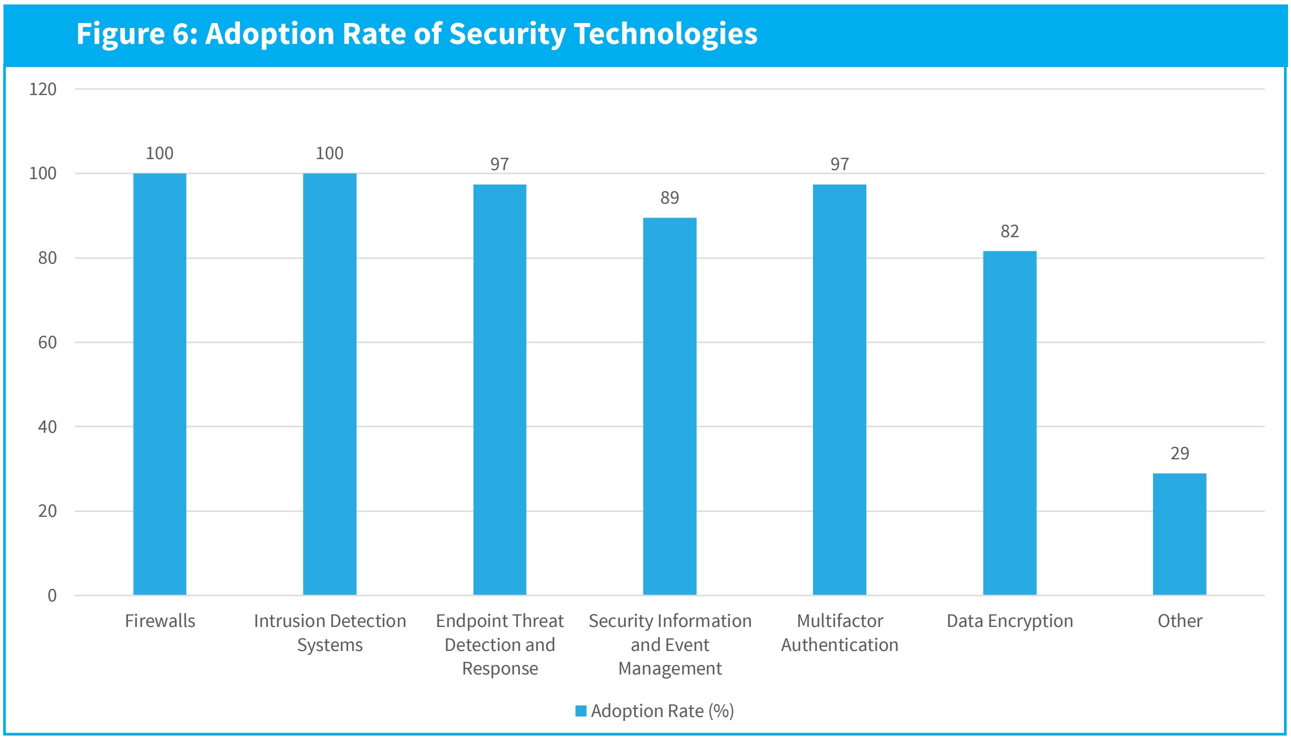
- The survey also sought to understand which security technologies are currently implemented by banks, aiming to assess the maturity and breadth of their cybersecurity infrastructure. By examining both widely adopted and more specialized tools, the findings provide valuable insight into how financial institutions are responding to evolving cyber threats and strengthening their overall security posture.

- Firewalls and Intrusion Detection Systems (IDS) have been universally adopted, with all banks (100 percent) implementing these foundational technologies. Endpoint Threat Detection and Response and Multifactor Authentication follow closely at 97 percent. Security Information and Event Management (SIEM) is slightly less prevalent, as reported by 89 percent of commercial banks, while Data Encryption is implemented by 82 percent of commercial banks.

- While the core technologies are well-represented, 29 percent of institutions reported using additional security tools not included in the standard options. These ***other*** technologies reflect more advanced and targeted capabilities. These include:

  - Privileged Access Management (PAM).
  - Web Application Firewalls (WAF).
  - Database Activity Monitoring (DAM).
  - Network Access Control (NAC).
  - Email Security Solutions.
  - Threat Intelligence Platforms.
  - Distributed Denial of Service (DDoS) Protection.
  - Mobile Device Management (MDM).
  - File Integrity Monitoring (FIM).
  - Security Orchestration and Automation (SOAR).
  - Hardware Security Modules (HSM).

Figure 6: Adoption Rate of Security Technologies



- This pattern indicates a growing trend towards layered and specialized cybersecurity solutions, particularly among banks with more mature and proactive security strategies.

3.7 Impact and Challenges

- Commercial banks that have adopted the CBK Cybersecurity Guidance 2017 noted that it significantly:
  - Strengthened their cybersecurity governance and risk management.
  - Improved incident response capabilities and resilience.
  - Enhanced regulatory and compliance framework.
  - Improved cybersecurity resilience through initiatives such as setting up security operations center (SOC).
  - Increased capacity building and awareness on cybersecurity.
  - Improved security controls by implementing secure configuration baselines for IT systems.
  - Increased assurance on the systems and technical infrastructure supporting the banking sector.
- Commercial banks noted the following challenges that they faced during the implementation of the Cybersecurity guidelines. These challenges included the following:
  - Risk management of Artificial Intelligence solutions.
  - Reliance on manual monitoring due to limited technology to provide real-time security visibility and monitoring to address emerging threats.
  - Continuous increase in the cost of cybersecurity maintenance.
  - Evolving cyber threat landscape.
  - High-cost of technical training and tools.

  - High cost of attracting, retaining and motivating cybersecurity experts due to the shortage of cybersecurity experts.

- The respondents recommended the following emerging areas to be included in the Guidance:
  - Artificial Intelligence and machine learning concerns from a cybersecurity perspective.
  - Cloud computing and the corresponding governance framework.
  - Application programming interface security.
  - Cyber risk insurance and risk transfer mechanisms.
  - Enhanced controls on mobile money fraud detection.
  - Managing data protection related risks.
  - Threat intelligence sharing mechanism could be captured in the guidance note, once a framework has been developed to support anonymized intelligence sharing.
  - Third party cybersecurity guidelines and controls compliance.
  - Regulatory framework for zero trust architecture.
  - Digital identity.
  - Internet of things security.

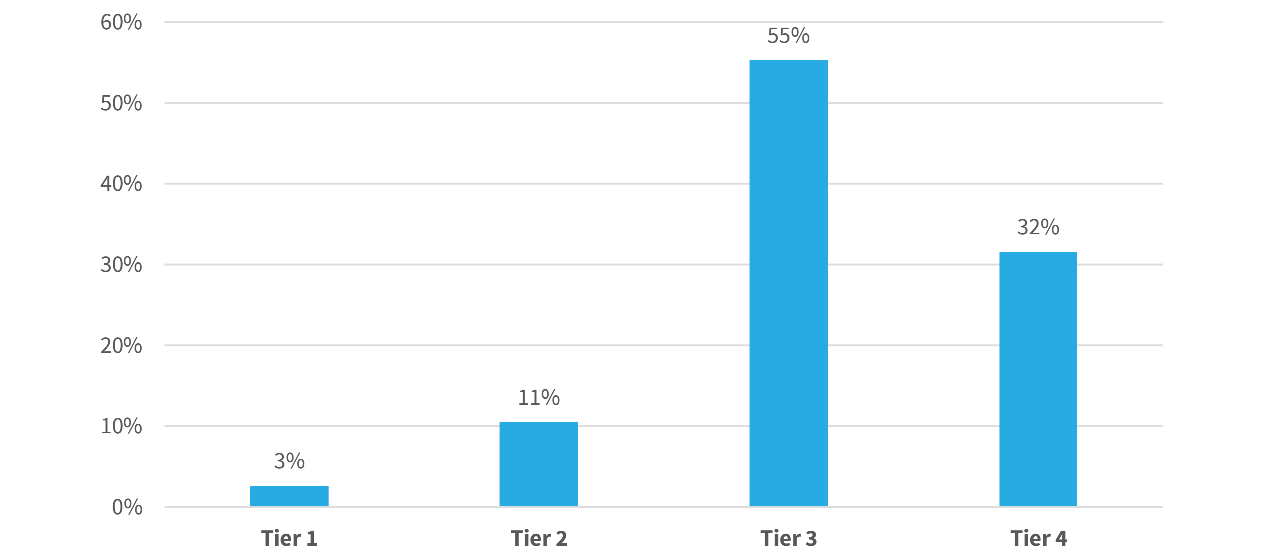
3.8 Cybersecurity Maturity Assessment

- The survey also assessed the maturity of the bank's cybersecurity framework, outlining the methodologies, models, criteria, and tools used to evaluate and enhance its cybersecurity posture.
  - NIST Cybersecurity Framework (CSF) is the most widely adopted, used by 63 percent of commercial banks. It serves as a foundational model for structuring and evaluating cybersecurity risk.
  - ISO/IEC 27001 is employed by 47 percent of commercial banks, offering a formal information security management system-based approach for continual improvement in cybersecurity.
  - Capability Maturity Model Integration (CMM/CMMI) is used by 26 percent of commercial banks to assess cybersecurity capabilities across predefined maturity levels.
  - Cybersecurity Capability Maturity Model (C2M2) is mentioned by 8 percent of commercial banks as a tool for identifying gaps and enhancing cybersecurity capabilities.
  - COBIT (Control Objectives for Information and Related Technologies) is used by 11 percent of commercial banks, primarily for governance and audit integration.
  - Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, tailored for financial institutions, is used by 3 percent of commercial banks.
- 53 percent of the respondents apply more than one framework concurrently, combining tools such as NIST, ISO 27001, CMMI, and others to achieve a more holistic view of cybersecurity maturity.

- Commercial banks supplement internal evaluations with external audits, cybersecurity consultants, or benchmarking exercises against global standards such as SWIFT Customer Security Programme (CSP), Payment Card Industry Data Security Standard (PCI-DSS), and local regulations (e.g., CBK Cybersecurity Guidelines 2017, Kenya Data Protection Act).
- 3 percent of commercial banks reported having no formal cybersecurity maturity assessment process in place, highlighting an area for immediate attention.
- Banks reported evaluating their cybersecurity maturity based on:
    - o Governance and risk management.
    - o Incident response readiness.
    - o Compliance with national and international regulations.
    - o Technical controls and system monitoring.
    - o Security awareness programs.
    - o Key performance indicators (e.g., time to detect/respond, user awareness)
    - o Business continuity and third-party risk management.

3 percent of commercial banks considered their cyber maturity level as "Tier 1", 11 percent as "Tier 2", 55 percent as "Tier 3" and 32 percent as "Tier 4". The tiers characterize the rigor of an organization's cybersecurity risk governance practices and risk management practices.[1]

Figure 7: Cyber Maturity Level



[1] *Tier 1 – Application of the organizational cybersecurity risk strategy is managed in an ad hoc manner. Prioritization is ad hoc and not formally based on objectives or threat environment.*

Tier 2 – Risk management practices are approved by management but may not be established as organization wide policy. The prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business requirements.

Tier 3 – The organization's risk management practices are formally approved and expressed as policy. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape.

Tier 4 – There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. Executives monitor cybersecurity risks in the same context as financial and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances.

3.9 General Comments

The respondents indicated that the 2017 CBK Guidance on Cybersecurity had a positive impact by helping them protect sensitive data, prevent cyberattacks, and maintain operational continuity. The Guidelines establish best practices for securing networks, systems, and user behaviour, reducing vulnerabilities, and minimizing the risk of breaches. By promoting awareness and accountability, these guidelines have enhanced trust among customers, partners, and stakeholders, while also ensuring compliance with legal and regulatory standards.

4.0 RECOMMENDATIONS

Recommendations for Banks

- Appoint and Empower CISOs: All banks should prioritize appointing a Chief Information Security Officer (CISO), with sufficient authority and resources to lead cybersecurity strategy and operations.
- Enhance Risk Assessment Frequency: Standardize and increase the frequency of cyber risk assessments, aiming for at least quarterly reviews to remain responsive to the evolving threat landscape.
- Integrate Cyber Budgeting: Ensure dedicated and visible cybersecurity budgeting, separate from general IT budgets, to reflect the criticality and strategic nature of cybersecurity.
- Adopt Layered Security Technologies: Invest in advanced security tools such as Distributed Denial of Service (DDoS) protection, Threat Intelligence Platforms, and zero-trust architectures.
- Formalize Cyber Maturity Evaluations: Institutionalize cybersecurity maturity assessments using global frameworks like NIST CSF, ISO 27001, and CMMI, and benchmark results against industry peers.
- Implement a comprehensive third-party cybersecurity risk framework covering due diligence, monitoring, and compliance requirements for vendors, especially in cloud and API environments.
- Establish or enhance Security Operations Centers (SOCs) with real-time monitoring capabilities.
- Conduct regular tabletop exercises and simulations to test incident response and business continuity plans.
- Expand cybersecurity training programs to include third-party service providers and integrate role-based awareness programs to address varied levels of access and responsibilities.

Recommendations for the Regulator (CBK)

- Review and update the 2017 CBK Cybersecurity Guidelines to address emerging risks such as:
  - Artificial Intelligence and Machine Learning
  - Cloud computing governance
  - API security
  - Zero trust architecture
  - IoT and mobile money fraud controls
  - Cyber insurance and risk transfer frameworks
  - Threat intelligence sharing and anonymized reporting
  - Digital identity protection and management
- Require banks to submit evidence of maturity assessments, including framework(s) used, maturity level ratings, and improvement plans.

- Consider mandating minimum cyber maturity tiers (e.g., Tier 3 or higher) for regulated institutions, with timelines for reaching compliance.

- Introduce cybersecurity key performance indicators (KPIs) for routine supervisory reviews (e.g., time to detect/respond, patch cycle time, user awareness rates).

- Conduct sector-wide cybersecurity stress tests or red-team exercises annually in partnership with external assessors.

- Facilitate inter-bank threat intelligence sharing through appropriate platforms.

- Organize periodic cybersecurity forums or workshops to promote awareness of current threats, best practices, and innovations.

- Support talent development initiatives, such as scholarships, internships, and public-private partnerships to grow local cybersecurity expertise.

Recommendations for Other Stakeholders

Kenya Bankers Association (KBA)

- Coordinate sectoral cybersecurity initiatives, such as joint training, shared threat intelligence, and standard vendor assessment templates.

- Develop a cybersecurity maturity roadmap to guide banks in achieving consistent standards.

- Collaborate with academia and training institutions to develop banking-specific cybersecurity curricula.

Technology Vendors and Third Parties

- Align their solutions and processes with CBK regulatory expectations, particularly regarding:
    - o Data protection compliance.
    - o Continuous monitoring and threat detection.
    - o Incident reporting protocols.
- Ensure transparency in security controls, auditability, and support for secure integration with banks' systems (e.g., APIs).

5.0 CONCLUSION

Cybersecurity threats have continued to evolve and become more complex, with increased frequency of threats such as phishing, ransomware, Distributed Denial-of Service (DDoS) attacks, amongst others. Consequently, financial institutions are required to proactively secure their critical information assets to ensure that they remain resilient in the face of these persistent threats. The prevalence of the use of emerging technology by financial institutions to deliver services to customers has also increased their attack surface. Commercial banks have highlighted emerging technology areas that CBK should consider incorporating into the Guidance on Cybersecurity.

As cyber threats evolve in scale and sophistication, updated guidance from Central Banks plays a critical role in safeguarding the stability, trust, and integrity of the financial system. Accordingly, CBK has embarked on the process of updating the 2017 CBK Guidance on Cybersecurity to commercial banks.

ANNEX 1: GLOSSARY OF TERMS

- **Artificial Intelligence** – is a technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.
- **Chief Information Security Officer (CISO)** – 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.
- **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.
- **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.
- **Cybersecurity incident** – is any malicious act or suspicious event that: compromises, or attempts to compromise, the electronic security perimeter or physical security perimeter of a critical Cyber Asset or disrupts or attempts to disrupt, the operation of a critical Cyber Asset.
- **Cybersecurity Maturity Tiers** – As part of cybersecurity maturity assessments, financial institutions are categorized into four tiers (Tier 1 to Tier 4) based on the sophistication of their cybersecurity risk management practices. The table below provides a description of what each tier entails, offering a structured benchmark for evaluating an institution's cybersecurity readiness.

Scenarios[2]	Description
Tier 1	• There is limited awareness of cybersecurity risks at the organizational level. • The organization implements cybersecurity risk management on an irregular, case-by-case basis. • The organization may not have processes that enable cybersecurity information to be shared within the organization. • The organization is generally unaware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses.
Tier 2	• There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. • Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. • Cybersecurity information is shared within the organization on an informal basis. The organization is aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks.

[2] *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*

Scenarios[2]	Description
Tier 3	• There is an organization-wide approach to managing cybersecurity risks. • Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. • The organization consistently and accurately monitors the cybersecurity risks of assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risks. Executives ensure that cybersecurity is considered through all lines of operation in the organization. • The organization risk strategy is informed by the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Personnel formally act upon those risks through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.
Tier 4	• There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. • Executives monitor cybersecurity risks in the same context as financial and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. • The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. • The organization uses real-time or near real-time information to understand and consistently act upon the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. • Cybersecurity inform`1ation is constantly shared throughout the organization and with authorized third parties.

- **Data Encryption** – refers to the process of converting data from a readable, plaintext format into an unreadable, encoded format: ciphertext. Users and processes can only read and process encrypted data after it is decrypted. The decryption key is secret, so it must be protected against unauthorized access.

- **Distributed Denial of Service** (DDoS) – refers to a malicious cyberattack where an attacker floods a target website or service with excessive traffic from multiple sources, making it unavailable to legitimate users.

- **Endpoint Threat Detection and Response** – refers to a cybersecurity technology that continually monitors an "endpoint" (e.g. a client device such as a mobile phone, laptop, Internet of things device) to mitigate malicious cyber threats.

- **Firewall** – describes a security device that monitors and controls network traffic between a trusted network and an untrusted network. It regulates incoming and outgoing network traffic based on preset security rules.

- **Intrusion Detection System (IDS)** – describes an application that monitors network traffic and searches for known threats and suspicious or malicious activity. The IDS sends alerts to IT and security teams when it detects any security risks and threats.

- **Machine Learning** – is a subset of Artificial Intelligence that enables systems to learn and improve from experience without explicit programming. It uses algorithms to analyze data, identify patterns, and make predictions or decisions.

- **Security Information and Event Management** – refers to a software solution that gathers and analyzes security data from various sources across an IT infrastructure, allowing organizations to identify and respond to potential security threats in real-time by correlating events and detecting anomalies across different systems.

- **Security Operations Centre (SOC)** – this refers to a centralized function within an organization that monitors, detects, prevents, and responds to cyber threats. It's essentially a team of security professionals who work 24/7 to protect the organization's IT infrastructure and data from cyberattacks.

ANNEX 2: LIST OF RESPONDENTS

Commercial Banks and Mortgage Finance Institution

1. Absa Bank Kenya Plc.
2. Access Bank (Kenya) Plc.
3. African Banking Corporation Limited.
4. Bank of Africa Kenya Limited.
5. Bank of Baroda (Kenya) Limited.
6. Bank of India.
7. Citibank N.A. Kenya
8. Consolidated Bank of Kenya Limited.
9. Co-operative Bank of Kenya Limited.
10. Credit Bank Plc.
11. Development Bank of Kenya Limited.
12. Diamond Trust Bank Kenya Limited.
13. DIB Bank Kenya Limited.
14. Ecobank Kenya Limited.
15. Equity Bank Kenya Limited
16. Family Bank Limited.
17. First Community Bank Limited.
18. Guaranty Trust Bank (Kenya) Limited.
19. Guardian Bank Limited.
20. Gulf African Bank Limited.
21. Habib Bank A.G Zurich.
22. HFC Limited.
23. I&M Bank Limited.
24. KCB Bank Kenya Limited.
25. Kingdom Bank Limited.
26. Mayfair CIB Bank Limited.
27. Middle East Bank Kenya Limited.
28. M-Oriental Bank Limited.
29. National Bank of Kenya Limited.
30. NCBA Bank Plc.
31. Paramount Bank Limited.
32. Prime Bank Limited.
33. SBM Bank Kenya Limited.
34. Sidian Bank Limited.
35. Stanbic Bank Kenya Limited.
36. Standard Chartered Bank Kenya Limited.
37. UBA Kenya Bank Limited.
38. Victoria Commercial Bank Limited.

Central Bank of Kenya

Haile Selassie Avenue P.O. Box 60000 - 00200 Nairobi | Tel: (+254) 20 - 286 0000 / 286 1000 / 286 3000

www.centralbank.go.ke | www.facebook.com/CentralBankKenya | @CbkKenya