BANKI KUU YA KENYA

GUIDELINE ON CYBERSECURITY

FOR PAYMENT SERVICE PROVIDERS

JULY 2019

GUIDELINE ON CYBERSECURITY FOR PAYMENT SERVICE PROVIDERS

ANNEXES

PART I: PRELIMINARY

1.1 Title – Guideline on Cybersecurity for Payment Service Providers (PSPs)

1.2 Authorization - This Guideline is issued pursuant to Section 31(2) (b) of the National Payment System Act, 2011, which empowers the Central Bank of Kenya (CBK) to issue Directives and Guidelines to be adhered to by Payment Service Providers in order to maintain a sound, secure and efficient National Payment System.

1.3 Application – The Guideline applies to all Payment Service Providers authorized under the National Payment System Act, 2011.

1.4 Definitions – The acronyms and some of terms used in this Guideline are defined below:

1.4.1 'Business Continuity' is a state of continued and uninterrupted operation of business.

1.4.2 '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 operational, financial, legal, reputational and other material consequences arising from disruption.

1.4.3 '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.

1.4.4 'CISO' is an acronym referring to the Chief Information Security Officer. He/ She is the senior-level executive within a PSP responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

1.4.5 '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 payment service providers and the economy.

1.4.6 'Cybersecurity Incident' is a cyber event that:

i. jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or

ii. violates the security policies, security procedures or acceptable use policies,

iii. whether resulting from malicious activity or not.

1.4.7 'Critical Asset' means facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of an institution.

1.4.8 'Cyber Asset' means programmable electronic devices and communication networks including Hardware, Software and Data.

1.4.9 'Critical Cyber Asset' means programmable electronic devices and communication networks including Hardware, Software and Data that are essential to the reliable operations of critical assets.

1.4.10 'Cybercrime' refers to a harmful activity executed through computers, Information Technology (IT) systems and/or the internet using a computer device as the tool to commit the offence, and targeting the computers, IT infrastructure or internet presence of another person or entity.

1.4.11 'Cybersecurity' means preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

1.4.12 'Cyber risk' is the combination of the probability of cyber incidents occurring and their impact.

1.4.13 'Cyberspace' is a global domain within the information environment consisting of the independent network of information systems infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

1.4.14 'Data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

1.4.15 'Designated Payment Instrument' means any payment instrument that is of widespread use as a means of making payment and may affect the payment systems of Kenya and it is thus designated to protect the interest of the public or in the interest of the integrity of the payment instrument.

1.4.16 'Designated Payment System' means any system that poses systemic risk or that is designated to protect the interest of the public or the interest of the integrity of the payment system.

1.4.17 'Endpoint' means a point in place and time at which payment instruction information is exchanged between two parties in the ecosystem, such as between a messaging network and a participant in the network, a payment system and a participant in the system or a payment system and a messaging network. Endpoint does not relate solely to parties at either end of a payment transaction chain, but rather participants of wholesale payment systems or messaging networks that can transmit and receive payment instructions on behalf of themselves and others.

1.4.18 'Endpoint Hardware' may include mobile devices, laptop or desktop personal computers (PCs) and other equipment such as servers and network devices that may or may not be controlled directly by the operator of a payment system or messaging network.

1.4.19 'External Dependency Management Strategy (EDMS)' is the strategy which provides for the protection and sustainment of the PSP's services and assets that are dependent on the actions of external actors e.g. technology vendors, suppliers, shared public infrastructure, and other external services that supports the PSP.

1.4.20 'Internal Dependency Management Strategy (IDMS) is the strategy which ensures that the PSP is able to identify and deal with cyber risks associated with its internal business environment e.g. workforce, data, technology, facilities etc. upon which the PSP depends to deliver services to its customers.

1.4.21 '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.

1.4.22 'Operator' means a person, other than a designated payment system operator, authorized in terms of section 8 (2) (c) of the National Payment Systems Act, 2011 to provide services to any two or more persons in respect of payment instructions.

1.4.23 'Participant' means a bank or institution approved by Central Bank of Kenya to participate in the Kenya wholesale payment system.

1.4.24 'Payment Service Provider (PSP)' as defined in the National Payment Systems Act, 2011 means:

i) A person, company or organization acting as provider in relation to sending, receiving, storing or processing of payments or the provision of other services in relation to payment services through any electronic system;

ii) A person, company or organization which owns, possesses, operates, manages or controls a public switched network for the provision of payment services; or

iii) Any other person, company or organization that processes or stores data on behalf of such payment service providers or users of such payment services.

1.4.25 'Retail Payment Systems' means a funds transfer system that typically handles a large volume of relatively low-value payments in such forms as cheques, credit transfers, direct debits and card payment transactions.

1.4.26 '**Social Engineering'** is a general term for trying to deceive people into revealing information or performing certain actions.

1.4.27 'Systemically Important Payment System (SIPS)' means a funds transfer system that typically handles large-value and high-priority payments. These are typically Wholesale or Large Value Payment System (LVPS). A failure of these systems could potentially endanger the operation of the whole economy. SIPS typically clear and settle high-value, time-sensitive wholesale payments (e.g. bank-to-bank transfers). A disruption or failure in a SIPS has the potential to pose the greatest risk to the financial stability and economic activity, safety and soundness of the national payment system.

1.4.28 'System-Wide Important Payment Systems (SWIPS)' means retail payment systems which are of importance to the economy as a whole due to the high volumes, low values of transactions they process, but which are unlikely to generate or transmit financial shocks if they fail. Such systems, however, are widely used and have poor short-term substitutes. Disruption of SWIPS services may not lead to financial instability but can create widespread disruptions due to the large number of users relying on the system, thereby affecting public confidence.

1.4.29 'Third Party Service Provider' means a person/entity that

(i) is not an affiliate of the PSP,

(ii) provides services to the PSP, and

(iii) maintains, processes or otherwise is permitted access to confidential information through its provision of services to the PSP.

PART II: STATEMENT OF POLICY

2.1 Purpose

The Guidelines outline the minimum requirements that PSPs shall build upon in the development and implementation of strategies, frameworks, policies, procedures and related activities aimed at mitigating cyber risk. The purpose of this Guideline therefore, is to:

(i) Create a safer and more secure cyberspace that underpins information system security priorities, to promote stability of the Kenyan payment system sub-sector;

(ii) Establish a coordinated approach to the prevention and combating of cybercrime;

(iii) Up-scale the identification and protection of Critical Information Infrastructure (CII);
(iv) Promote compliance with appropriate technical and operational cybersecurity standards;
(v) Guide PSPs in developing the 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
(vi) Help maintain public trust and confidence in the National Payment System.

2.2 Scope

This Guideline sets the minimum standards that PSPs 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 PSPs 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 Sources of Cyber Risk

Cyber-attacks launched against organizations' information systems have placed the abuse of cyberspace high in the domestic as well as the international agenda. Some illustrations of sources of cybercrime activities include but are not limited to: -

(i) Unauthorized 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.
(ii) People related attacks like phishing, malware introduced through social engineering that can be utilized to gain privileged access to critical systems.
(iii) Interconnectedness of institutions could lead to compromise in the institutions' entry points such as through service providers.
(iv) 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.
(v) Poor authentication controls to protect customer data, transactions and systems.

2.4 Responsibility

The board of directors and senior management of payment service providers are expected to formulate and implement cybersecurity strategies, frameworks, policies and procedures, which must be documented and made available for review by external auditors and CBK. The board of directors is ultimately responsible for the cybersecurity of the PSP.

2.5 Cybersecurity Program

Each PSP shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the PSP's Information Systems. The cybersecurity program shall be based on the PSP's risk assessment and designed to perform the following core cybersecurity functions:

(i) Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of confidential information stored on the PSP's information Systems;
(ii) Use defensive infrastructure and the implementation of policies and procedures to protect the PSP's Information Systems, and the confidential information stored on those information systems, from unauthorized access, use or other malicious acts;
(iii) Detect cybersecurity events;
(iv) Respond to identified or detected cybersecurity events to mitigate any negative effects;
(v) Recover from cybersecurity events and restore normal operations and services;
(vi) Implement a comprehensive testing program to assess the effectiveness of the cybersecurity program;
(vii) Utilize cyber threat intelligence and information sharing mechanisms to understand the cyber threat environment within which an institution is operating; and
(viii) Fulfill applicable regulatory reporting obligations.

PART III: SPECIFIC REQUIREMENTS

3.1 Governance of PSPs

3.1.1 Board of Directors

The board members of a PSP should understand the nature of their PSP's business and the cyber risks to which the PSP can be exposed. Robust oversight and engagement on cyber risk matters at the board level promotes a security risk conscious culture within the PSP. Specifically, 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 PSP's vision, risk appetite and overall strategic direction with regards to cybersecurity. Cybersecurity should be incorporated as part of the general risk assessment of the PSP. The Board shall approve the PSP's cybersecurity risk acceptance and risk assessment.
(iii) Allocation of adequate budget to cybersecurity activities based on the PSP's information systems complexity.
(iv) Assign a CISO the responsibility for reporting to the Board regularly, but not less than once per quarter, on the PSP's cybersecurity posture and progress in implementing the cybersecurity strategy and goals.
(v) Review management's determination of whether the PSP's cybersecurity preparedness is aligned with its cyber risk profile. Include cybersecurity strategies in procedures and policies of the PSP and train all employees with digital access on security policies and procedures.

(vi) Establish or review cybersecurity risk ownership and the management's accountability. The coverage should include relevant business lines and not just the IT function. Identify employees responsible for cybersecurity in the organization.

(vii) Approve and review on a regular basis the implementation of the PSP's cybersecurity program, frameworks, policies, strategies and procedures, including the adequacy of existing mitigating controls, and ensure cybersecurity audits and infrastructure vulnerability tests are performed. The review should be done at least once in 12 months.

(viii) Put in place adequate cybersecurity monitoring structures with an escalation matrix to senior management with accountability of the Board.

(ix) Review the results of management's ongoing monitoring of the PSP's exposure to and preparedness for cyber threats and implementation of user security awareness programs.

(x) Ensure that the Board has members with appropriate skills and knowledge to understand risks posed by cyber threats and ensure those skills remain current and the Board is kept abreast of cybersecurity developments.

3.1.2 Senior Management

Senior Management of a PSP is responsible for implementing the PSP's business strategy in line with its risk appetite, while being cognizant of cyber 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.

(iv) Continuously improve collection, analysis, and reporting of cybercrime information. This can be achieved through understanding the business environment the PSP operates 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.

(vii) Incorporate cybersecurity as an agenda in senior management meetings and provide regular reports of the PSP's cybersecurity posture to the board.

(viii) Document a cybersecurity incident response plan providing a roadmap for the actions the PSP 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.

(ix) Create a post incident analysis framework to determine corrective actions to prevent similar incidents in the future.

(x) Oversee the evaluation and management of risks introduced by third party service providers to the PSP.

(xi) The role of senior management should extend to include:

a) Ensuring that cybersecurity processes are conducted in line with business requirements, applicable laws and regulations.

b) When a PSP or its agent becomes aware of cybersecurity incident involving a potential or actual data breach either in any of its systems or environments or in the systems or environments of its agent(s), the PSP must take (or cause the agent to take) the following actions:

- Immediately commence a thorough investigation into the data breach or potential data breach.
- Immediately, or within a reasonable time, identify, contain, and mitigate the data breach or potential data breach.

3.1.3 Chief Information Security Officer (CISO)

(i) As cyber-attacks evolve, one of the modern strategic measures globally accepted and acknowledged is the introduction of the role of the CISO. This role is aimed at creating an organizational culture of shared cybersecurity ownership. All PSPs are required to have a CISO.

(ii) The PSP should determine the best reporting option of the CISO depending on factors such as the PSP'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. The CISO could report to either the Chief Executive Officer (CEO), Chief Information Officer (CIO), Chief Operating Officer (COO) or Risk Function. Where a CISO reports to the CIO, the institution should ensure that there are compensating controls to ensure the CISO's independence and prevent conflict of interest. Such controls should include:

a) Regular, independent reporting to the board of directors on the institution's cybersecurity posture.

b) Independent budget approved by the board of directors.

(iii) The CISO is responsible for:

a) Developing and implementing the PSP's cybersecurity program and enforcing the cybersecurity policy.

b) Ensuring that the PSP maintains a current and comprehensive cyber asset and user register.

c) Ensuring that the PSP's cybersecurity strategy addresses the needs of the PSP, taking into account the overall business strategies, risk appetite and ICT risk management policies of the PSP.

d) 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).

e) Organizing professional cyber related trainings to improve technical proficiency of staff and user awareness trainings for improved cyber hygiene.

f) Ensure that adequate processes are in place for monitoring IT systems to detect cybersecurity events and incidents in a timely manner.

g) 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 PSPs.
   - 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 PSP during the period.

h) Reporting to the Board on an agreed interval but not less than once per quarter on the PSP's capability to manage cybersecurity and progress in implementation of the cybersecurity strategy and goals.

i) Ensure timely update of the incident response mechanism and Business Continuity Plan (BCP) based on the latest cyber threat intelligence gathered.

j) Incorporate the utilization of scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.

k) Ensure adequate backups of critical IT systems and data in line with predetermined recovery objectives (e.g. real time back up of changes made to critical data) are carried out to a site that is unlikely to be affected by a disaster event at the main processing site.

l) 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.

m) Put in place BCP and disaster recovery test plans to ensure that the PSP can continue to function and meet its regulatory obligations in the event of an unforeseen attack through cyber-crime.

n) Assessing the overall effectiveness of the PSP's cybersecurity program.

o) Periodically reporting on the organization's cybersecurity posture to senior management, board and audit committee.

(iv) Where a PSP seeks to use a third party provider to perform the responsibilities outlined in Clause 3.1.3 (c), the PSP should only consider outsourcing operational security functions such as information security monitoring, testing and threat intelligence. A PSP may not outsource governance, oversight and management functions of the CISO. Where a PSP seeks to use a third party service provider to support the CISO operational security functions, the PSP shall seek prior approval of CBK. In such a case, the PSP shall:

a) retain responsibility for compliance with this clause;

b) designate a senior member of the PSP's personnel responsible for direction and oversight of the third party service provider; and

c) require the third party service provider to maintain a cybersecurity program that protects the PSP in accordance with the requirements of this clause.

3.1.4 Cybersecurity Strategy, Frameworks and Policies

Each PSP shall implement and maintain a written policy or policies, approved by the PSP's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the PSP's policies and procedures for the protection of its information systems and confidential information stored on those Information Systems. The cybersecurity policy shall be based on the PSP's risk assessment and address the following areas to the extent applicable to the PSP's operations:

(i) Information security.
(ii) Data governance and classification.
(iii) Asset inventory and device management.
(iv) Access controls and identity management.
(v) Business continuity and disaster recovery planning and resources.
(vi) Systems operations concerns.
(vii) Systems and network security.
(viii) Systems and network monitoring.
(ix) Systems and application development and quality assurance.
(x) Physical security and environmental controls.
(xi) Customer data privacy.
(xii) Vendor and third party service provider management.
(xiii) Risk assessment.
(xiv) Incident response.

3.2 Risk Management

3.2.1 Risk Assessment

Each PSP shall conduct a periodic risk assessment of the PSP's information systems sufficient to inform the design of the cybersecurity program as required by this clause. Such risk assessment shall be updated as reasonably necessary, but not less than once a year, to address changes to the PSP's information systems, confidential information or business operations.

The PSP's risk assessment shall allow, among others, for the identification of critical cyber assets and revision of controls to respond to technological developments and evolving threats. The assessment shall consider the particular risks of the PSP's business operations related to cybersecurity, confidential information collected or stored, information systems utilized and the availability and effectiveness of controls to protect confidential information and information systems.

The board of directors shall be required to approve the risk assessment and risk acceptance. The risk assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(i) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the PSP;

(ii) criteria for the assessment of the confidentiality, integrity, security and availability of the PSP's information systems and confidential information, including the adequacy of existing controls in the context of identified risks; and

(iii) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

3.2.2 General Risk Management Requirements for PSPs

A PSP should establish a robust operational risk-management framework with appropriate systems, policies, procedures and controls to identify, monitor and manage operational risks.

(i) A PSP's management should clearly define the roles and responsibilities for addressing operational risk and should endorse the PSP's operational risk-management framework

(ii) Systems, operational policies, procedures and controls should be reviewed, audited and tested annually for critical cyber assets and once every two years for other assets and after significant changes.

(iii) A PSP should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.

(iv) A PSP system should have comprehensive physical and information security policies that address all major vulnerabilities and threats.

(v) A PSP should have a business continuity plan that addresses events posing a significant risk of disrupting operations. The plan should be designed to protect end users' information and payment data and to enable recovery of accurate data following an incident. The plan should also seek to mitigate the impact on end users following a disruption by having a plan to return to normal operations.

(vi) A PSP should identify, monitor, and manage the risks that end users, participants, other PSPs, service and utility providers might pose to its operations.

(vii) In addition, a PSP should identify, monitor, and manage the risks that its operations might pose to others.

(viii) A PSP should strive to ensure compliance to international standards and best practices relating to account data compromise, breaches and cyber threats.

3.2.3 Dependency Risk Management

The understanding of the cyber threat landscape for the PSP requires a collaborative approach between its internal and external stakeholders. Proper understanding of the cyber threat landscape will therefore require the implementation of risk management strategies in the areas highlighted hereunder:

a) Internal Dependency Management

The PSP should have an explicit Internal Dependency Management Strategy (IDMS) integrated into the overall strategic and cyber risk management plan. This requires that the PSP has:

(i) Effective capabilities to identify and manage cyber risks associated with its business assets throughout their lifespans and to continually assess and improve as necessary, their ability to reduce the cyber risks associated with internal dependencies on an enterprise-wide basis.

(ii) A current and complete awareness of all internal assets and business functions that support the PSP's cyber risk management strategy.

(iii) An inventory of all business assets on an enterprise-wide basis, prioritized by their criticality to the business functions they support, the firm's mission and the financial sector.

(iv) The ability to track connections among assets and cyber risk levels throughout assets' life cycles using relevant data and analysis across the firm.

(v) Appropriate controls to address inherent cyber risk in the firm's assets, taking into account prioritization of the PSP's assets and the cyber risks they pose to the firm.

b) External Dependency Management

The PSP should have an explicit External Dependency Management Strategy (EDMS) which is integrated into the overall strategic and cyber risk management plan. This requires that the PSP has among other things:

(i) Effective capabilities in place to identify and manage cyber risks associated with external dependencies and interconnection risks throughout such relationships, and continually assess and improve as necessary, their effectiveness in reducing cyber risks associated with external dependencies and interconnection risks enterprise-wide;

(ii) The ability to monitor in real time all external dependencies and trusted connections that support the PSP's cyber risk management strategy;

(iii) A current, accurate and complete awareness of all external dependencies and trusted connections enterprise-wide, prioritized based on their criticality to the business functions they support, including mappings to supported assets and business function;

(iv) The ability to monitor the universe of external dependencies that connect to assets supporting systems critical to the PSP, the sector, as well as track connections among external dependencies, organizational assets, and cyber risks throughout their lifespans; and

(v) Tracking capabilities that enable timely notification of cyber risk management issues to designated stakeholders.

3.2.4 Incident Response and Cyber Resilience

(i) A cybersecurity incident is deemed to have occurred under circumstances that include, but are not limited to any of the following:

a) a PSP or its agent is informed, through any source, of the installation or existence of any malware in any of its systems or environments, or any system or environment of one of its agents, no matter where such malware is located or how it was introduced;
b) a PSP or its agent receives notification from CBK, or any other credible source that the PSP or its agent(s) has experienced a data breach or a potential data breach; or
c) a PSP or its agent discovers or, in the exercise of reasonable diligence, should have discovered a data breach or unauthorized penetration of its own system or environment or the system or environment of its agent(s).

(ii) The PSP should plan for, respond to, contain and be able to rapidly recover from disruptions caused by cyber incidents, thereby strengthening their cyber resilience. The PSP should therefore have the capability of operating critical business functions in the face of attacks and while continuously enhancing cyber resilience. An incident response plan shall address the following areas:

a) The internal processes for responding to a cybersecurity event;
b) The goals of the incident response plan;
c) The definition of clear roles, responsibilities and levels of decision-making authority;
d) External and internal communications and information sharing;
e) Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
f) Documentation and reporting regarding cybersecurity events and related incident response activities; and
g) The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

(iii) In addition, PSPs should:

a) Establish processes designed to maintain effective situational awareness capabilities to reliably predict, analyze and respond to changes in operating environment and to maintain effective incident response and cyber resilience governance.
b) Establish processes for secure offline storage of critical records, including financial records of the PSP using defined data standards to allow for restoration of the records after a disruption.
c) Conduct testing that addresses a disruptive, destructive, corruptive or any other cyber event that could affect the ability to service customers and avoid incurring significant downtime that would affect the business operations of customers.

3.2.5 Vulnerability Assessments and Penetration Testing

The cybersecurity program for each PSP shall include monitoring and testing, developed in accordance with the PSP’s Risk Assessment, designed to assess the effectiveness of the PSP’s cybersecurity program. The monitoring and testing shall include continuous monitoring and periodic Penetration Testing and Vulnerability Assessments.

In the absence of an effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in information systems that may create or indicate vulnerabilities, PSP's shall conduct:

(i) quarterly vulnerability scans of all critical cyber assets;

(ii) annual Penetration Testing of the PSP that cover, at a minimum, the critical cyber assets as determined each given year based on the Risk Assessment; and

(iii) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the PSP's Information Systems based on the Risk Assessment.

3.3 Additional Requirement for Systemically Important Payment Systems and System-wide Important Payment Systems

Operators of Systemically Important Payment Systems and System-Wide Important Payment Systems are required to:-

(i) Ensure that the CISO is a senior management officer that reports to the Board.

(ii) Work closely with their third-party service providers and other participants in the ecosystem to maintain and improve the security of interconnections and endpoint security. For example, an operator could conduct response and recovery tests with its third-party service providers and other participants.

(iii) Implement a Computer Security Incident Response Team (CSIRT), whether in-house or outsourced, that is responsible for responding to security incidents and intrusions, and coordinating activities among the relevant internal and external stakeholders. Such a team should have the authority to direct the operator to make the changes necessary to recover from the incident.

(iv) Conduct scenario-based tests that cover breaches affecting multiple portions of the operator's ecosystem in order to identify and analyse potential complexities, interdependencies and possible contagion both at business and operational level, which should be taken into account in the operator's cyber resilience framework.

3.4 Outsourcing

PSPs 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. PSPs should therefore ensure that their third-parties service providers comply with legal and regulatory frameworks as well as the international best practices. Generally, PSPs should:

(i) Have in place adequate governance framework for outsourcing agreements including due diligence on prospective service providers, documented outsourcing agreements and adequate monitoring of service delivery.

(ii) Consider all IT-related outsourcing agreements as critical infrastructure for regulation and protection for purposes of security of the payment systems industry and the economy at large.

(iii) Select their vendors based on compliance and risk assessments.

(iv) Ensure all outsourcing contracts require service providers to comply with applicable legal and regulatory frameworks.

(v) Periodically assess the PSP’s outsourced services to understand those which pose higher risk to the PSP so as to work with the third party on mitigation.

(vi) Have a documented data breach response plan that considers the third party and ensure that this is tested on a periodic basis. The results of the breach exercise should be shared with Senior Management, audit committee and the Board (as relevant).

(vii) Make it mandatory for their outsourced providers to report security incidents/breaches within a certain timeframe in line with best practice. Typically, 48 hours is a good benchmark.

(viii) Ensure the outsourced service or infrastructure is accorded at least the same minimum security standards that the PSP accords to non-outsourced services and infrastructures.

(ix) Ensure that Service Level Agreements should have robust provisions in relation to security, service availability, performance metrics and penalties.

3.4.1 Outsourcing Contracts

Outsourcing agreements should be governed by a clearly written contract, the nature and detail of which should be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the PSP. The agreement should also bring out the nature of legal relationship between the parties, that is, whether agent-principal or otherwise. Some of the key provisions of the contract include:

(i) Security incident reporting, the PSP’s and CBK’s right to audit the service provider, and penalty clauses for security lapses.

(ii) Details of activities to be outsourced including appropriate service and performance standards.

(iii) Controls to ensure customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information.

(iv) Contingency plans to ensure business continuity and periodic testing of these plans.

(v) A clause to allow CBK or persons authorized by it to access the institution’s documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. The agreement should further provide that in the event these are not made accessible CBK within a reasonable time, CBK may pursue any or all of the remedial actions and administrative sanctions provided for under the NPS Act.

3.4.2 Notification to CBK

PSPs should notify CBK of the intention to outsource functions, services and infrastructures at least thirty days before such outsourcing agreements are executed.

3.5 Regular Independent Assessment and Testing

PSPs should also carry out regular independent assessment and audit functions that shall be undertaken by the internal and external audit and risk functions.

3.5.1 Role of Risk Management Function

This comprises risk, control, compliance and oversight functions which ultimately ensure that the PSP'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 PSP'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 PSP'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 PSP to ensure appropriate control design.
(iv) Maintain comprehensive cyber risk registers. The PSP should identify and assess key cybersecurity risks regularly. 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.

3.5.2 Role of Internal Audit Function

PSPs should incorporate qualified Information and Communication Technology (ICT) auditors within their internal audit team. The ICT audit function can be outsourced if needed. The PSP's internal ICT auditors should ensure that the audit scope includes and is not limited to the tasks below:

(i) Regular review and report on cyber risks and controls of the ICT systems within the PSP and third party service providers.
(ii) Conduct up-front due diligence to mitigate risks associated with third parties.
(iii) Assess both the design and effectiveness of the cybersecurity framework implemented.
(iv) Conduct regular independent threat and vulnerability assessment tests.
(v) Report to the board the findings of the assessments.
(vi) Oversee the regular penetration tests and vulnerability scans.

3.5.3 Role of External Audit Function

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

(i) Obtaining an understanding of the PSP's IT infrastructure, use of IT, operations and the impact of IT on financial reporting statements.

(ii) Understanding the extent of the PSP's automated controls as they relate to business reporting for the PSP. This should include an understanding of:
   a) IT general controls that affect the automated controls.
   b) Reliability of data and reports used in the audit that are produced by the PSP.

(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 PSP's board and CBK on the findings of the assessments.

3.6 Training and Awareness

(i) PSPs should implement IT security awareness training programs to provide information on good IT security practices, common threat types and the PSP's policies and procedures. The training should be provided to all employees including senior management and the board.

(ii) A formalized plan should be put in place to provide ongoing technical training to cybersecurity specialists within the PSP.

(iii) Cybersecurity awareness and information should be provided to the PSP's customers, clients, suppliers, partners, outsourced service providers, staff and other third parties who have links to the PSP's IT infrastructure.

4.0 Transitional Periods

PSPs shall have 90 days from the effective date of this Guideline to comply with the requirements set forth in this Guideline.

PART IV: REPORTING

(i) 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 all PSPs are required to review their cybersecurity strategy, policy, and framework annually based on each PSP's threat and vulnerability assessment. All PSPs are required to submit their Cybersecurity Policy, Strategies and Frameworks to the CBK by December 31, 2019. This will not apply to commercial banks that are licensed under the Banking Act, who are subject to the Guidance Note on Cybersecurity (August 2017). High level contents of a cybersecurity policy are outlined in **Annex I** to this Guideline.

(ii) PSPs should notify CBK within 24 hours, and SWIPS and SIPS within 2 hours, of any Cybersecurity incident(s) that could have a significant and adverse impact on the PSP'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. This should be followed by a comprehensive report on the incident.

(iii) On a quarterly basis, PSPs 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.

The above information should be submitted to e-mail: nps@centralbank.go.ke In the event of any query or clarification, please contact:

The Director,
Banking and Payment Services Department
Central Bank of Kenya
P. O. Box 60000 - 00200,
Nairobi
Tel: 2860000
Email: nps@centralbank.go.ke

ANNEX I

HIGH LEVEL CONTENTS OF A CYBERSECURITY POLICY

The Cybersecurity Policy should generally contain the following:

(i) **Governance:** Mechanisms put in place to establish, implement and review its approach to managing cyber risks.

(ii) **Identification:** Operational failure can negatively impact financial stability hence the PSPs are required to identify their critical business functions and supporting information assets so as to safeguard them against compromise.

(iii) **Protection:** Cyber resilience depends on effective security controls that protect the confidentiality, integrity and availability of its assets and services.

(iv) **Detection:** PSP's ability to detect the occurrence of anomalies and events indicating a potential cyber incident is essential to strong cyber resilience. Early detection provides the PSP with useful lead time to mount appropriate counter measures against a potential breach, and allows proactive containment of actual breaches.

(v) **Resumption:** This relates to response and recovery and provides guidance on how a PSP should respond in order to contain, resume and recover from successful cyber-attacks.

(vi) **Testing:** Once employed within a PSP, the elements of its cyber resilience framework should be rigorously tested to determine their overall effectiveness.

(vii) **Situational awareness:** Strong situational awareness can significantly enhance a PSP's ability to understand and pre-empt cyber events, and to effectively detect, respond to and recover from cyber-attacks that are not prevented.

(viii) **Learning and evolving:** PSPs should aim to instill a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the PSP. 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.

(ix) **Collaboration:** Effective solutions may necessitate collaboration between the PSPs 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.

(x) **Organization and Resources:** Allocation of an adequate cybersecurity budget based on the PSP's structure and size of its cyber risk function.

(xi) **Cybersecurity Incident Management:** Cybersecurity incident response plan should provide a roadmap for the actions the PSP 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 of Incident	Time of Incident	Nature of Incident (Chronological order of events)	Impact Assessment

Submit the cybersecurity incident report after a cybersecurity incident(s) within 24 hours for PSPs and within 2 hours for SWIPS and SIPS, to the Director, Banking & Payment Services Department:

Email: nps@centralbank.go.ke
Signed for and on behalf of …………………………………………………………….
By the duly authorized Signatories
Name…………………………………………………………
Designation ……………………………………………………….
Signature ……………………………………………………

Name…………………………………………………………
Designation ……………………………………………………….
Signature ……………………………………………………

ANNEX III

CYBERSECURITY INCIDENT RECORD (QUARTERLY)

(*Insert Name of participant)* …………………………...……………………….………

(Reporting Period): …………………………………………………………….……………

No.	Date of Incident	Time of Incident	Nature of Incident	Action Taken	Time of Resolution	Action Taken to mitigate future incidents

Submit the cybersecurity incident report on the 10th day after the end of every quarter to the Director, Banking & Payment Services Department at email: nps@centralbank.go.ke
Signed for and on behalf of …………………………………………………………………………
By the duly authorized Signatories

Name……………………………………………………………………………………...

Designation ………………………………………………………….…………………………...

Signature …………………………………………………………………………………...

Name…………………………………………………………….……………………………..

Designation ……………………………………………………………………………………

Signature …………………………………………………………………………………………