GUIDELINES ON CYBERSECURITY

FOR PAYMENT SERVICE PROVIDERS

AUGUST 2018

TITLE: GUIDELINE ON CYBERSECURITY

PART I Preliminary

1.1 Title
1.2 Authorization
1.3 Application
1.4 Definitions

PART II Statement of Policy

2.1 Purpose
2.2 Scope
2.3 Sources of Cyber Risk
2.4 Responsibility

2.5 **PART III Specific Requirements**

3.1 Categories of Payment Service Providers
3.2 Governance of PSPs
3.3 General Risk Management Requirements for PSPs
3.4 Dependency Risk Management Strategies & Cyber Resilience
    3.2.1 Internal Dependency Management
    3.2.2 External Dependency Management
    3.2.3 Incident Response and Cyber Resilience

3.5 Regular Independent Assessment and Testing
    3.5.1 Role of Risk Management Function
    3.5.2 Role of Internal Audit function
    3.5.3 Role of External Auditors

3.6 Outsourcing
3.7 Training/Awareness

PART IV Reporting

ANNEXES

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

PART I: PRELIMINARY

1.1. Title – Guidelines on Cybersecurity

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 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. However, exemptions on certain requirements shall be identified based on the type and nature of a PSP.

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 operations, 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 an institution 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 provider and the economy.

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

1.4.7 'Cybercrime' according to the International Organization of Securities Commissions (IOSCO), 'cyber-crime' refers to a harmful activity executed by an individual or a group, through computers, Information Technology (IT) systems and/or the internet and targeting the computers, IT infrastructure or internet presence of another entity.

1.4.8 '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 access or modification, or exploitation.

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

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

1.4.11. '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.

1.4.12. '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.

1.4.13 'External Dependency Management Strategy (EDMS)' is the strategy which provides for the protection and sustainment of the institution'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 institution.

1.4.14 'Internal Dependency Management Strategy (IDMS) is the strategy which ensures that the institution 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 institution depends to deliver services to its customers.

1.4.15 '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.

1.4.16 'Payment Service Provider' is as defined in the National Payment System Act, 2011.

1.4.17 'Red Team Exercise' refers to an all-out attempt to gain access to a system by any means necessary, and usually includes cyber penetration testing, physical breach, testing all phone lines for modem access, testing all wireless and systems present for potential wireless access, and also testing employees through several scripted social engineering and phishing tests. These are real life exercises carried out by an elite small team of trained professionals that are hired to test the physical, cyber security, and social defenses of particular systems.

1.4.18 '**Social Engineering'** the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

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, policies, procedures and related activities aimed at mitigating cyber risk. The purpose of this Guidance Note therefore, is to:

- Create a safer and more secure cyberspace that underpins information system security priorities, to promote stability of the Kenyan payment system sub-sector;
- Establish a coordinated approach to the prevention and combating of cybercrime;
- Up-scale the identification and protection of critical information infrastructure (CII);
- Promote compliance with appropriate technical and operational cybersecurity standards;
- 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
- 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 institutions must comply with as part of their regulatory obligations, particularly in the areas of risk management, outsourcing, information communication technology, internal controls and corporate governance.

2.3 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 cybercrime activities include but not limited to: -

- A breach of institutions' databases exposing its data to cyber criminals.
- 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.
- People related attacks like phishing, malware introduced through social engineering that can be utilized to gain privileged system access to critical systems.
- Interconnectedness of institutions could lead to compromise in the institutions' entry points such as through service providers.
- Internal IT systems can themselves be a source of cyber risk. For example, data replication arrangements that are meant to safeguard business continuity could transfer malware or corrupted data to the backup systems.

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

2.4. Responsibility

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

PART III: SPECIFIC REQUIREMENTS

3.1 Categories of Payment Service Providers

For purposes of this Guideline PSPs are categorized into two broad types depending on the level of business operations such as volumes, values and requirement to hold trust funds accounts etc. Below are the 2 categories:

(a) Wholesale or Large Value Payment Systems (LVPS)

These are Systemically Important Payment Systems (SIPS). The disruption or failure in a SIP has the potential to pose the greatest risk to the financial stability and economic activity, safety and soundness of the national payment system. LVPS which clears and settles high-value, time-sensitive wholesale payments (e.g. bank-to-bank transfers), requires to be designated as a SIP and should be owned, operated and overseen as per the rules set by the Bank.

(b) Retail Payment Systems

The retail payment sector includes a wide array of payment service providers that vary in size and business model. The communication, compliance-assessment and remedial tools that are effective for one type of PSP, may not be optimal for other types of PSPs such as digital wallet providers, credit and debit card networks etc.

In this Guideline consideration will be given for PSPs posing a lower level of risk and classified as entities firms falling under a certain threshold and would be subject to less stringent requirements. For example, Firms could be tiered on different dimensions such as functions (e.g. holding funds), payments values or volumes, market significance (e.g. number of end users) and the degree of interconnectedness with other payment systems. Smaller firms could be permitted to self-assess the operational reliability of their internal systems, while the larger firms could be required to conduct third-party assessments.

3.2 Governance of PSPs

a) Board of Directors

The board members of a PSP should understand the nature of their institution's business and the cyber risks to which the institution can be exposed. Robust oversight and engagement on cyber risk matters at the board level promotes a security risk conscious culture within the institution. 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. The institution of sound cybersecurity strategy and framework

iii. Engage management in establishing the institution's vision, risk appetite and overall strategic direction with regards to cybersecurity.

iv. Allocation of adequate budget to cybersecurity activities based on the institution's information systems' complexity.

v. Review management's determination of whether the institution's cybersecurity preparedness is aligned with its cyber risk profile.

vi. Adoption of an effective internal cybersecurity control framework with submission of periodic independent reports.

vii. Establish or review cybersecurity risk ownership and the management's accountability. The coverage should include relevant business lines and not just the IT function.

viii. Review on a regular basis the implementation of the institution's cybersecurity framework and implementation plan, including the adequacy of existing mitigating controls. The review should be done at least once in 12 months.

ix. Include the reporting of cybersecurity as a standard agenda in Board meetings.

x. 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.

b) Senior Management

Senior Management of an institution 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 institution 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) Ensure timely and regular reporting to the board on the cyber risk status of the institution.

viii) Incorporate cybersecurity as a standard agenda in Senior Management meetings and provide regular reports of the PSP's cybersecurity posture to the board.

ix) Document 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:
   - The roles and responsibilities of staff;
   - Incident detection and assessment, reporting; and
   - Escalation and strategies deployed.

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

xi) Oversee the evaluation and management of risks introduced by third party service providers; PSP's may require attestation/assurance reports provided by reputable independent auditors for service providers.

c) Chief Information Security Officer (CISO)

As cyber-attacks evolve, one of the modern strategic measures globally accepted and acknowledged is the introduction of the role of the Chief Information Security Officer (CISO). This role is aimed at creating an organizational culture of shared cybersecurity ownership.

Where this is applicable the institution should determine the best reporting option of the CISO depending on factors such as the institution's vision and strategic goals, culture, management style, security maturity, IT maturity, risk appetite and all relevant dynamics involving the current security posture and reporting lines. The CISO should report to either the Chief Executive Officer (CEO), Chief Information Officer, Chief Operating Officer or Risk Function. Most importantly is to ensure that the CISO serves in the Senior Management Team.

The CISO is responsible for:

i) Overseeing and implementing the institution's cybersecurity program and enforcing the cybersecurity policy.

ii) Ensuring that the PSP maintains a current enterprise-wide knowledge base of its users, devices, applications and their relationships.

iii) Ensuring that information systems meet the needs of the PSP 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 PSP.

iv) Design cybersecurity controls with the consideration of users at all levels of the organization, including internal (i.e. management and staff) and external users (i.e. contractors/consultants, business partners and service providers).

v) Organizing professional cyber related trainings to improve technical proficiency of staff.

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

vii) Reporting to the CEO on an agreed interval but not less than once per quarter on the following:
   - Assessment of the confidentiality, integrity and availability of the information systems in the institutions.

- Detailed exceptions to the approved cybersecurity policies and procedures.
- Assessment of the effectiveness of the approved cybersecurity program.
- All material cybersecurity events that affected the PSP during the period.

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

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

x) 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.

xi) 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.

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

d) Exemption from the Requirements

Notwithstanding the requirements as stated above, and in recognition of the different types and varying operational capacities of PSPs and the need to encourage innovation in the payment sector, certain types of PSPs such as small e-money issuers and Fintech innovators posing limited risk to end users would be exempted from the requirements of having a CISO. However, such institutions are required to conduct adequate self-assessment tests for operational reliability of their internal systems and submit the report to CBK on a bi-annual basis.

3.3 General Risk Management Requirements for PSPs

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

ii) 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

iii) Systems, operational policies, procedures and controls should be reviewed, audited and tested periodically and after significant changes.

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

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

vi) 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.

vii) A PSP should identify, monitor, and manage the risks that end users, participants, other PSPs, and service and utility providers might pose to its operations. In addition, a PSP should identify, monitor, and manage the risks that its operations might pose to others.

3.4 Dependency Risk Management Strategies and Cyber Resilience

The understanding of the cyber threat landscape for the institution 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:

3.4.1 Internal Dependency Management

The institution 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 enterprise-wide basis,
ii) A current and complete awareness of all internal assets and business functions that support the institution'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) 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 PSP's assets and the cyber risks they pose to the firm.

3.4.2 External Dependency Management

The institution 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 institution'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 firm and sector, and 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

3.4.3 Incident Response and Cyber Resilience

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. The PSP should therefore, among other things:

i) 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.
ii) Establish processes for secure offline storage of critical records, including financial records of the institution using defined data standards to allow for restoration of the records after a disruption.
iii) 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.

3.5 Regular Independent Assessment and Test

PSPs should also carry out regular independent assessment and testing of following functions: Internal Audit, Risk Management and External Audit.

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: Key cybersecurity risks should be regularly identified and assessed. Risk identification should be forward looking and include the security incident handling.
v) Ensure implementation of the cyber and information risk management strategy.
vi) Safeguarding the confidentiality, integrity and availability of information.

vii) Ensure that a comprehensive inventory of IT assets, classified by business criticality, is established and maintained. A Business Impact Analysis process is in place to regularly assess the business criticality of IT assets.

viii) Quantify the potential impact by assessing the residual cyber risk and considering risks that need to be addressed through insurance as a way of transferring cyber risk.

ix) Reporting all enterprise risks consistently and comprehensively to the board to enable the comparison of all risks equally in ensuring that they are prioritized correctly.

x) Conduct red team exercises.

3.5.2 Role of Internal Audit Function

PSPs should incorporating qualified information and communication technology (ICT) auditors within their Internal Audit team. ICT audit function can be outsourced or through internal placement. The PSP's internal ICT auditors should therefore ensure that the audit scope includes and is not limited to the tasks below:

i) Continuous review and report on cyber risks and controls of the ICT systems within the PSPs and other related third-party connections.

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) Conduct comprehensive penetration tests.

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 institution'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:

- IT general controls that affect the automated controls.
- 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 institution's board and CBK on the findings of the assessments.

3.6 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 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) Analyze the PSP's outsourced services to understand those which pose the most relative higher risk to the institution so as to work with the third party to mitigate the risk.

vi) Monitor contracted third parties for changes in their business and cyber security posture including expansions, divestitures, breaches and new attacks that may alter the third parties' exposure. Service Level Agreements should have robust provisions in relation to security, service availability, performance metrics or penalties.

vii) Ensure that the outsourcing contract provides that the CBK can exercise its oversight and supervisory powers in respect of the NPS Regulations.

viii) Notify the CBK of the intention to outsource functions at least thirty days before such outsourcing agreement execution.

ix) Develop exit management strategies and contingency plans.

3.7 Training/Awareness

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

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 institution's customers, clients, suppliers, partners, outsourced service providers and other third parties who have links to the PSP's IT infrastructure.

PART IV: REPORTING

a) CBK is well aware of the fact that cyber risk will keep morphing due to the evolution of cyber threats in Kenya and across the globe. The Bank therefore requires all Payment Service Providers (PSPs) to periodically review their cybersecurity strategy, policy, and framework regularly based on each PSP's threat and vulnerability assessment. All PSPs are required to submit their Cybersecurity Policy, Strategies and Frameworks to the Central Bank of Kenya by August 31, 2018. High level contents of a cybersecurity policy are outlined in **Annex I** to this Guideline.

b) The Payment Service Providers should notify the Central Bank of Kenya within 24 hours of any Cybersecurity incident(s) that could have a significant and adverse impact on the 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.

c) On a quarterly basis, Payment Service Providers 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 & 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:

- **Governance:** Mechanisms put in place to establish, implement and review its approach to managing cyber risks
- **Identification:** Operational failure can negatively impact financial stability hence the financial institutions are required to identify their critical business functions and supporting information assets so as to safeguard them against compromise.
- **Protection:** Cyber resilience depends on effective security controls that protect the confidentiality, integrity and availability of its assets and services.
- **Detection:** 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.
- **Resumption:** This relates to response and recovery and provides guidance on how a PSP institution should respond in order to contain, resume and recover from successful cyber-attacks.
- **Testing:** Once employed within a PSP, the elements of its cyber resilience framework should be rigorously tested to determine their overall effectiveness.
- **Situational awareness:** Strong situational awareness can significantly enhance a 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.
- **Learning and evolving:** PSP should aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the 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.
- **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.
- **Organization and Resources:** Allocation of an adequate cybersecurity budget based on the PSP's structure and size of its cyber risk function.
- **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 within 24 hours after a cybersecurity incident(s) 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 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 ……